Volume 11

Pages 2104 - 2291

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

Before The Honorable James Donato, Judge

IN RE GOOGLE PLAY STORE ANTITRUST LITIGATION,	**NO. 21-md-02981-JD**
THIS DOCUMENT RELATES TO:	
EPIC GAMES, INC., Plaintiff,	
VS.	**NO. 3:20-cv-05671-JD**
GOOGLE, LLC., et al., Defendants.	

San Francisco, California
Tuesday, November 21, 2023

TRANSCRIPT OF PROCEEDINGS

STENOGRAPHICALLY REPORTED BY:

Kelly Shainline, CSR 13476, RPR, CRR
Official United States Reporter

APPEARANCES:

For Plaintiff:

CRAVATH, SWAINE & MOORE LLP
825 Eighth Avenue
New York, New York 10019
BY: GARY BORNSTEIN, ATTORNEY AT LAW
YONATAN EVEN, ATTORNEY AT LAW
LAUREN MOSKOWITZ, ATTORNEY AT LAW
MICHAEL ZAKEN, ATTORNEY AT LAW
BRENT BYARS, ATTORNEY AT LAW
ANDREW WIKTOR, ATTORNEY AT LAW

For Defendants:

MUNGER, TOLLES & OLSON LLP
350 South Grand Avenue - 50th Floor
Los Angeles, California 90071
BY: GLENN POMERANTZ, ATTORNEY AT LAW
KURUVILLA J. OLASA, ATTORNEY AT LAW
NICK R. SIDNEY, ATTORNEY AT LAW

MUNGER, TOLLES & OLSON LLP
601 Massachusetts Avenue NW
Suite 500 East
Washington, DC 20001
BY: JONATHAN KRAVIS, ATTORNEY AT LAW
LAUREN BELL, ATTORNEY AT LAW

MORGAN, LEWIS & BOCKIUS LLP
One Market - Spear Street Tower
San Francisco, California 94105
BY: MICHELLE PARK CHIU, ATTORNEY AT LAW

I N D E X

Tuesday, November 21, 2023 - Volume 11

E X H I B I T S

Tuesday - November 21, 2023 **9:08 a.m.**

P R O C E E D I N G S

---000---

(Proceedings were heard out of the presence of the jury:)

THE COURT: We're all set. Bring them out.

(Proceedings were heard in the presence of the jury:)

THE CLERK: Calling Civil 20-5671, Epic Games, Inc. vs. Google LLC, and Multidistrict Litigation 21-2981, In re Google Play Store Antitrust Litigation.

Counsel.

MR. BORNSTEIN: Good morning, Your Honor. Gary Bornstein for Epic Games. Today I have Brent Byars, Michael Zaken, Andrew Wiktor, Lauren Moskowitz, and Yonatan Even.

MR. POMERANTZ: Good morning, Your Honor. Glenn Pomerantz on behalf of Google, and with me today is Michelle Park Chiu, Lauren Bell, Lara Kollios, Nick Sidney, Jonathan Kravis, and Kuru Olasa.

THE COURT: Okay. So let's talk a little bit about long-range planning. All right? We're making excellent progress.

Fact witnesses are going to end today for Epic; right?

MR. BORNSTEIN: Correct, Your Honor.

THE COURT: Okay. And then we're going to do the experts.

Now, we have been talking internally here about having

court on December 1st, a week from Friday. Let's plan on that because I want to get this done.

And remember, I said this during jury selection but let me remind you, we're going to be dark the week of the 5th. So if anybody has anything happening the week of the 5th, you'll probably be okay, but we're not going to be here the week of the 5th. All right?

So it will be December -- sorry -- the week of the 4th. I guess it's Monday the 4th. So the 4th through the 9th, whatever those four days are, five days are, we'll be done -- not in. So if you have something to do, you can probably do it.

And then on the 11th we'll be back, and then we'll be very close to closing and deliberations at that point. Okay?

All right. Okay. Go ahead. Who -- oh, we have the Amazon fellow?

MR. BORNSTEIN: Yes, Your Honor. We'll continue with Mr. Morrill.

THE COURT: Okay.

(Video was played but not reported.)

THE COURT: Okay. Who's next?

MR. BORNSTEIN: Your Honor, we have one more deposition to play. This is the Spotify witness. And we have an agreed method, subject to your approval, just to implement Your Honor's rulings on confidentiality.

THE COURT: Okay.

MR. BORNSTEIN: There are three Q and As where we propose to just mute the video and turn off the transcript, and we have handouts for Your Honor and for the jury just to read those three Q and As when they come up.

THE COURT: All right.

MR. BORNSTEIN: Thank you, Your Honor.

And we have just two exhibits to move into evidence as well as to which there's no objection.

THE COURT: So we're a courtroom of the people of the United States. We do our business in the sunshine so everyone can see what's going on, particularly in antitrust cases which affect a broad variety of people.

There are some very limited occasions when there's a compelling reason to protect some information. I think this is the first time -- it might be the second time -- we're doing it in this case. So you will see it. It just won't be broadcast to the rest of the courtroom. Okay? That's what we're talking about.

Thank you.

MR. BORNSTEIN: And for the record while things are being passed out, the witness' name is Sandra Alzetta, A-L-Z-E-T-T-A.

THE COURT: Okay. Go ahead.

MR. BORNSTEIN: Your Honor, we would move the

admission of Exhibits 1532 and 2062.

MR. KRAVIS: No objection.

THE COURT: All right. They're admitted.

(Trial Exhibits 1532 and 2062 received in evidence.)

MR. BORNSTEIN: Thank you.

(Video was played but not reported.)

THE COURT: Stop.

Did that work out? Yeah?

Okay. Go ahead.

(Video continuing playing but not reported.)

THE COURT: Okay. We'll take our morning break and come back at 10:45.

THE CLERK: All rise.

(Recess taken at 10:28 a.m)

(Proceedings resumed at 10:47 a.m)

(Proceedings were heard out of the presence of the jury:)

THE COURT: Bring them in.

(Proceedings were heard in the presence of the jury:)

MR. CLARKE: Your Honor, my name is Justin Clarke on behalf of Epic Games, and Epic calls Professor James Mickens.

THE COURT: Oh, is this an expert? No other fact witnesses?

MR. BORNSTEIN: Your Honor, we have two video deposition fact witnesses together about a half an hour. We have some matters we're working out with Google to finalize

those so they can be played without issue --

THE COURT: Oh, okay.

MR. BORNSTEIN: -- and we're going to do them right before the accountants because they'll go together with the accounting testimony to facilitate everything.

THE COURT: Okay. Our first expert witness.

THE CLERK: Please stand and raise your right hand.

JAMES WILLIAMSON MICKENS,

called as a witness for the Plaintiff, having been duly sworn, testified as follows:

THE WITNESS: I do.

THE CLERK: Thank you. Please be seated.

THE WITNESS: Thank you.

THE CLERK: Please state your full name for the Court and spell your last name.

THE WITNESS: My full name is James Williamson Mickens, and my last name is spelled M-I-C-K-E-N-S.

THE CLERK: Thank you.

DIRECT EXAMINATION

BY MR. CLARKE:

Q. Good morning, Professor Mickens.

A. Good morning.

Q. What is your profession?

A. I'm a professor of computer science at Harvard University.

Q. And what subjects do you teach at Harvard?

A. I teach a class on operating systems, and I teach a class on computer security.

And, by the way, I've prepared some slides which will discuss my qualifications among other things. I'm not sure if people can see them. Okay. There they are.

Q. Thank you.

Could you tell us a little bit about your educational background?

A. Sure. So I got my bachelor's of computer science at Georgia Tech, and then I went to the University of Michigan also in computer science.

Q. Mr. Mickens, what did you do before you were teaching at Harvard?

A. Before I came to Harvard, I was a researcher in the Distributed Systems Research Group at Microsoft Research. So I did that for seven years. And I was also a visiting professor at MIT in their parallel and distributed operating systems group.

Q. Have you published any articles related to your research?

A. I have, yes. I try to publish in top-tier venues that discuss computer security, as well as the construction in the evaluation of large-scale software systems.

Q. Do you have any experience related to the area of mobile device security?

A. I do. So I've published several papers that look

specifically at issues of mobile security, for example, looking at the propagation of malware on mobile devices, as well as different secure ways to expose smartphone hardware devices, like GPS units or cameras to mobile web pages.

MR. CLARKE: Your Honor, Epic Games would like to offer Professor James Mickens as an expert in the area of mobile device security.

MR. OLASA: No objection, Your Honor.

THE COURT: He is qualified to testify on that topic.

BY MR. CLARKE:

Q. So, Professor Mickens, what were you asked to do in this case?

A. So if we go to the next slide, I discuss my assignment in this case. So my assignment was to evaluate Android security as it relates to app distribution mechanisms. And in particular, I was asked to examine whether the friction that Android imposes on non-Google Play Store app installation is justified by legitimate security concerns.

Q. And, Professor Mickens, when you use the term "friction," what do you mean by that?

A. By "friction" I just mean the screens, the dialogues, the warnings that an operating system is going to put up and show to users and sort of force the user to click through or interact with before the user can actually accomplish the intended task.

Q. And could you summarize your conclusions?

A. Sure. So if we go to the next slide.

So here I show a summary of my three conclusions, and so the first conclusion is that the friction that's imposed by an operating system during app installation should be proportional to the likelihood that the app is harmful. And the way that we would determine the likelihood that an app is harmful is by subjecting that app to a high-quality security review.

Q. What was your second conclusion?

A. So my second conclusion was that if you look at how friction is imposed on the Android system today, well, the friction that Google currently imposes to installing apps via third-party channels is unwarranted, and it's unwarranted because it's disproportionate to the security risks that are involved during those app installations.

Q. And, Professor Mickens, when you use the term "third-party channels," what do you mean by "third-party channels"?

A. Oh, so by that I just mean sort of non-preinstalled app stores.

Q. Okay. And did you reach any other conclusions?

A. I did. As we see up there on the slide, I reached a third and final conclusion, which is the following:

I think that by making small changes to the way that Android currently works, Google could actually reduce that unwarranted friction that users experience during the app

installation process while preserving or even strengthening the status quo of security on Android today.

Q. Thank you.

So could you preview for us the bases for those conclusions that you reached?

A. Sure. And so if we go to the next slide.

And so here I'm showing the bases for my conclusions. And so the first basis is an observation, and it's the observation that if you look at how Android is designed, apps from both first-party stores and third-party channels are subject to the same on-phone security measures. And that's important because that means regardless of where a user gets their apps from, the OS is still going to be there trying to protect the user.

Q. Okay. What were your other bases for your conclusions?

A. So if we look at that second basis, that's also another observation, and it's the observation that if you look at Google's own self-stated security goals -- right? -- according to their own security experts, those security goals do not treat installation from third-party channels as inherently more dangerous than installation from first-party channels. And that's important because if that's true, then we shouldn't be putting unnecessarily disproportionate friction on the installation of apps via third-party channels.

Q. Are there any other bases for your conclusions?

A. Yes. So we see that up on the slide.

So my third basis is another observation. So it's an observation that if you look at the machine-learning tools that Google uses to detect malware -- these are kind of like artificial-intelligence-type things that look at an app and try to tell if it's malicious -- well those machine-learning tools, they don't actually use the app's distribution channel when calculating the maliciousness score for that app. And that makes sense because the reason why an app would be malicious is not the distribution channel it came from, but whether what it tries to do to the user's phone.

Q. And when you say "distribution channel," what are you referring to?

THE COURT: You need to -- just pull that thing towards you.

MR. CLARKE: The microphone?

THE COURT: Yeah. Don't crane down. Just move it to you. Don't bring yourself to the soup. Bring the soup to you. Okay?

MR. CLARKE: Thanks, Your Honor.

THE COURT: Closer. I can tell it's not close enough.

MR. CLARKE: Is that better, Your Honor?

THE COURT: You're craning. Move it toward you like 4 inches. Yeah. A little more.

All right. Boom it out.

MR. CLARKE: How's that?

THE COURT: Yeah.

And, Professor, if you just slow down. We have a realtime court reporter, and just 20 percent slower, if you could.

THE WITNESS: Yes, Your Honor.

THE COURT: Okay. Go ahead.

MR. CLARKE: Thank you, Your Honor.

BY MR. CLARKE:

Q. So, Professor Mickens, I was asking you what you mean when you use the term "distribution channel."

A. Right. So when I talk about a distribution channel, I just mean a mechanism by which a user installs an app on their phone. So an app store via direct installation, so on and so forth.

Q. Can you describe your next basis for your conclusions?

A. Sure. So that's also up there on the screen.

So the fourth basis for my conclusions, it's another observation. And the observation is that according to Google's own employees, according to documents that are in production, we'll see that Google has actually underresourced its security monitoring of off-Play distribution channels. And that's really important because that means that when Google talks about the sort of larger risks of installation via these third-party channels, well, they've actually under resourced the policing of those channels.

Q. And did you have any other bases for your conclusions?

A. Yes. I had a fifth and final basis, which we also see up there on the screen.

So it's another observation. Once again, it's the observation that Google has the ability to identify and review apps at the point of installation.

And why is that important? That's important because, once again, it means that regardless of the installation channel by which apps arise on the user's -- arrive on the user's phone, Google can still determine whether those apps are malicious or not.

Q. So, Professor Mickens, what sources did you consider when you were preparing these opinions?

A. I list those sources on the next slide, so if we could go there.

So here are the five high-level types of sources that I relied upon when sort of handling my assignment.

The first source was Google's own source code. So you can think of these as sort of the instructions that Google developers generate when they're trying to make software like Android. So I looked at a variety of Google-provided source code.

I also looked at a variety of documents from Google that came out of the production process.

I looked at some deposition transcripts of Google employees.

I also examined Google's public statements to see, you know, sort of what they're telling users and developers just out there in the wild.

And, finally, I looked at academic articles where appropriate.

Q. Professor Mickens, you mentioned source code. Which specific types of source code did you look at?

A. So on the next slide I enumerate the specific source code that I looked at.

So there are three high-level categories of source code I looked at. The first involves the automated scanning of mobile apps. So this is the on-device malware scanner that's going to look for evidence that an app is trying to harm your machine.

I also looked at Google documentation involving how Android shows notifications to users.

I also looked at documentation about how Android handles signatures. So signatures are a cryptographic idea. They basically allow us to determine that a particular party saw a particular digital file, and they also allow us to make sure that nobody has tampered with that file.

And then the final piece of a source code that I looked at is the AOSP code. AOSP stands for Android Open-Source Project. You can think of AOSP as forming a big chunk of the Android operating system and, among other things, it provides important security properties.

Q. Okay. Thanks.

So you referred to the Android operating system. Could we start by explaining to the jury what the components of the Android operating system are?

A. Sure. So if we go to the next slide.

So what I'm showing you here is sort of a high-level overview of what an Android phone looks like. So all the way at the bottom we have the hardware. So these are the physical circuits and components like the touchscreen, the storage device, and so on and so forth.

Now, up at the top you have the user apps. So these are the apps that you engage with directly. This is your e-mail client. This is a game or something like that.

And then in the middle we have the actual Android operating system itself.

Q. Okay. And so there's a bar at the bottom here that says "AOSP Kernel." Do you see that?

A. I do.

Q. What is that?

A. So AOSP, once again, that stands for Android Open-Source Project. So this is code that is written and developed by Google. It forms sort of the bedrock of the Android operating system; and for the purposes of this case, probably the most important thing is that it implements a lot of the key security features that keep users safe.

Q. And above it in the upper left-hand corner there's a square that says "AOSP Middleware." Do you see that?
A. I do.
Q. And what's that?
A. So at a high level, middleware is kind of like the executive assistant for the kernel. So apps oftentimes don't submit requests directly to the kernel; they submit it to middleware. And so that middleware acts as that assistant.

So the AOSP middleware, those are sort of helpful functions that are part of AOSP, the project. So this is also code that is written and developed by Google.
Q. So on the right-hand side there's a square that says "OEM and SOC Middleware." Do you see that?
A. I do.
Q. And what does that refer to?
A. So that just refers to middleware that is written and developed by either the OEM, so that's basically the person who sells you the phone; and then the SOC, that stands for system on a chip, you can basically think of this as like the hardware vendor. So there's middleware that's provided by both the OEM and the hardware vendor.
Q. Okay. And, lastly, in the middle there's a square that says "GMS Middleware." Do you see that?
A. Correct.
Q. And what is the GMS middleware?

A. So GMS middleware, so what does GMS stand for? It stands for Google Mobile Services. So this is middleware that is also written and developed by Google. Unlike the AOSP contents of Android, GMS is closed source. Okay? So you can't just go out there and look and see what its contents are. So GMS middleware is distinct from that open-source AOSP middleware.

Q. And does GMS also include any user-facing apps that would appear kind of in that top row there?

A. It does. So it includes a couple different user-facing apps; and, actually, if we go to the next slide, I can sort of show you the breakdown of both the middleware and the user-facing apps that are shown.

So --

Q. Okay. Could you explain to us the left-hand column of this slide?

A. Yes. So on the left-hand column of the slide we're showing the middleware that is present inside of GMS. And so you'll see that there's middleware called Google Play Protect. You'll oftentimes see that abbreviated GPP. That is the on-device malware scanner. Okay? So that's what Google Play Protect is.

You'll also see "Package Installer" in that left-hand side. That's very important with respect to this case. Package Installer is Google-provided middleware that is going to orchestrate the process of installing an app and, in

particular, orchestrate that showing of friction screen. So Package Installer is a very important part of the GMS middleware.

Q. Great. Thank you.

And you referenced that there are some user-facing apps as well. What are those?

A. That's right. So if we look sort of in the little image of the touchscreen, we'll see a bunch of icons for apps, user-facing apps, that are part of GMS. These are just apps that correspond to popular Google services like Gmail, like YouTube. You'll also see the Play Store is there as well. So that's part of the GMS suite as well.

Q. So is it possible to market a phone that doesn't use any of the GMS functionality and relies only on AOSP functionality?

A. In theory, that's possible, and that's sort of what we're showing off to the right where we show a phone that only uses the AOSP middleware. It will still use Package Installer because that's part of the AOSP middleware and the GMS middleware; but if you look sort of in the touchscreen area, you'll see that the AOSP-only phone, it can't have Google apps like Chrome, it can't have Google apps like the Play Store because those are part of the GMS services.

Q. And do you have a general sense of how many phones out there, generally speaking, use GMS as opposed to AOSP only?

A. Yes. To the best of my knowledge, outside of the Chinese

market, all of the popular Android phones that we would all be familiar with in this courtroom, all of those are GMS-licensed phones, to the best of my knowledge.

Q. So if you're an OEM that wants to market some sort of a GMS phone, is there anything you need to do from a contractual perspective, to your knowledge?

A. There is. And so I explain this in the next slide.

So an OEM can't just take the GMS suite and just put that on the OEM's phone. Instead, the OEM has to engage in a bunch of contractual arrangements with Google.

In the upper right-hand corner we see two examples of those: The Mobile Application Distribution Agreement, sometimes called the MADA, and also the GMS requirements.

For the purposes of this case, probably the most important sort of contractual stipulation here is that the OEM is locked into using the Package Installer middleware. Remember, that's code written and developed by Google. The OEM is locked into using that middleware to orchestrate the app installation process on the phone. So that means that the OEM is locked into using that Google-mandated friction flow.

Q. Is there anything that the OEM has to do from a technical perspective in order to comply with the MADA and the GMS requirements?

A. Yes. So Google provides a series of automated tests or tools that verify whether the OEM's version of Android actually

satisfies requirements like, you know, using the right version of a Package Installer. That's what we see in the lower left-hand corner of the screen, Google Test Suites. So those are just automated pieces of code that look at the OEMs variant of Android and says "Have you satisfied, you know, the various contractual requirements?"

Q. So in the upper right-hand corner here there's something that says "Compatibility Definition Document." Do you see that?

A. I do.

Q. What is that?

A. So that is another example of a requirement that an OEM has to satisfy if they want to sell these GMS-licensed phones. That document, the CDD, Compatibility Definition Document, it enumerates other important characteristics of an Android phone.

Among other things, and perhaps most importantly at least for my assignment, that document defines the security properties, the sort of protections that an OEM's version of Android has to implement to keep users safe from potentially harmful apps.

Q. And is there anything technically that OEMs have to do in order to comply with the CDD?

A. Yes. So if we look in the lower right-hand corner, we see this Compatibility Test Suite or CTS. This is another set of automated tests that Google provides and which it will run on

an OEM's version of Android to make sure that that variant of Android actually satisfies the security properties and other properties specified by the CDD.

Q. So what is your understanding of the significance of all of this for security from Google's perspective?

A. Well, here I want to sort of present a quote that's from actual Google security engineers. So if we go to the next slide.

So this is a quote that's taken from an academic paper about security. It's a paper that is written by Google security engineers. And so what this paper says in that quote there, it says "Security is a compatibility requirement."

And so, you know, what does that mean? That means that as a result of all those requirements and tests that OEMs have to satisfy, any phone that claims that it is Android licensed and GMS certified has to implement a core set of security properties to prevent users from harm from malicious apps.

Q. So, Professor Mickens, I'd like to walk through how it is that apps can come to be on an Android phone.

Could you walk through the distribution channels for us?

A. Sure. So let's go to the next slide.

So, yeah, let's look at the different types of distribution channels, the different ways that apps can arrive on a user's phone.

So the first broad category of distribution channels

represents preinstalled app stores. So these are app stores that are sort of on the phone, you know, by the time that you buy it from whoever it is that sells the phone.

And so we see that the Play Store is an example of a preinstalled store, the first-party store in this case, and that's going to be mandatory on GMS devices. So that has to be on a GMS device.

Sometimes you will see other preinstalled stores. So, for example, on Samsung devices, you may see the Galaxy Store but those are not mandatory, and Google sometimes engages in sort of contractual disincentives to prevent those stores from showing up.

So long story short, on a GMS device, you're always going to see the Play Store preinstalled.

Q. Thank you.

And are there any other distribution channels available on the Android phones?

A. There are. So if we go to the next slide.

So here we see third-party app stores. Okay? And I'm specifically referring here to third-party app stores that are installed after the fact. So after you purchase the phone.

I just give two examples here. F-Droid is an example of one of them. Amazon Appstore is an example of one of them as well.

Q. Any other distribution channels that are available?

A. Yes. So if we hit next slide.

So here we see instances of what we call a direct installation. Sometimes you'll hear that referred to as sideloading. So direct installation just means that you are going to, as a user, find an app via a mechanism that is not billing itself purely as an app store.

So, for example, you might go to a developer's website via a browser like Chrome or Mozilla and find the app to install there. You might also find that in a file manager, something like that.

So that's what I mean when I say "direct installation."

Q. So, Professor Mickens, if a user wants to directly install an app from a website, how can they tell whether they're actually on the correct website and not some sort of a fake website?

A. So as it turns out, web browsers have a variety of mechanisms to try to make sure that users don't accidentally end up at a bad website. And so I give an example of this on the next slide. So if we can click through there.

So here what we're talking about is https. So you may have noticed that when you type in a URL. What does S stand for? It stands for secure.

And, among other things, what the browser is going to do when you go to a site, it's going to look and see: Is this site implementing that secure version of http? And if it

claims to do so, are there any problems with the way that that site keeps your data safe in terms of encrypting the network traffic?

And so here I just give you three examples of warning screens that you might get from three different browsers if you go to a site that isn't properly encrypting the data exchange between your browser and the server.

So this is just one example of how web browsers try to prevent issues with users going to harmful sites.

Q. So, Professor Mickens, you mentioned three different distribution channels. Can you tell us what Google's security goals indicate about those different distribution channels?

A. Right. So we talked about those three channels: Preinstalled app stores, postinstalled third-party app stores, and direct installation.

And if we go to the next slide, we can see what Google security engineers, from that paper that I mentioned earlier, think about this open ecosystem.

They say in this paper, which lays out the security goals for the Android platform, they say, quote (as read):

> "Both users and developers are part of an open ecosystem that is not limited to a single-application store."

So that's interesting; right? Because it says that, you know, Google security engineers responsible for designing the

security mechanisms in Android, they understand that open-ecosystem access is important and they understand that the security mechanisms they build into Android must protect users regardless of the distribution channel by which apps arrive on a user's phone.

Q. So I want to talk about the sorts of protections that Android phones have against malware.

Could you walk us through what sorts of security protections exist on the device itself?

A. Sure. So if we go to the next slide.

So what I'm showing you here are some of the security mechanisms that a phone provides at the hardware level. So, for example, there's this thing called encrypted data storage. This basically just means that your sensitive information on your device is kept in encrypted or scrambled form. So if some attacker takes your phone and later on wants to look at it, well, the thief isn't going to see anything reasonable. They'll see garbled data.

There's also a technique called verified booting, which prevents malware from tampering with the operating system or other important low-level pieces of software.

Q. Does the operating system itself provide any sorts of security protections against malware?

A. It does. And if we go to the next slide.

So here we see a bunch of different security mechanisms

that the Android OS itself provides. And so this is not an exhaustive list. There are a bunch of other security mechanisms that OS provides as well.

You know, just looking at a handful of the mechanisms on this slide: Storage sandboxing prevents one app from stealing data that belongs to another app.

If you look at device permissions, that means that if an app wants to use a sensitive piece of hardware on your phone, like the GPS unit or the camera, the OS forces the app to ask for permission, to ask for consent, before that app can access that device.

And so there's a bunch of other mechanisms there. I just want to point out that all of these mechanisms here, they're enforced regardless of whether user apps come from first-party or third-party distribution channels.

Q. Do Android phones do any sort of on-device malware scan?

A. They do. So if you go to the next slide.

So here you see Google Play Protect. So that's GPP, the GPP that I called out earlier. That is the on-device malware scanner, which is going to try to find harmful apps that are on your phone.

Q. So what is the relevance of these security mechanisms to the conclusions that you outlined at the beginning of your testimony this morning?

A. Well, if we go back to those conclusions, then as sort of

a key theme throughout all of those conclusions is that regardless of how an app gets on a user's phone, there are going to be very strong security protections that are applied by the hardware and particularly by the operating system, as well as by Play Protect as well.

And so what we see is that, from the perspective of security, regardless of where I get my apps from, first-party channels or third-party channels, there's this wide fleet of protections that are going to be applied regardless of those sources where I get apps from.

Q. And does the operating system treat some apps as more trusted than others based on where the apps came from?

A. No, it does not.

Q. Sundar Pichai, Google's CEO, testified last week that, quote (as read):

> "If users install by chance the wrong application, it gives full access to your operating system, all your data on the phone."

As a mobile device security expert, do you agree with that statement?

A. I do not agree with that statement.

Q. Why not?

A. Well, the reason is because of all of these security mechanisms that I just discussed. So even if a user does have the misfortunate to download a potentially harmful app on their

phone, there is still going to be all of these mechanisms in place trying to keep the user safe.

And so unless the malware is a particular type of malware that can somehow do, you know, what's called like a sandbox escape or a privilege escalation, unless the malware can do that, all of these mechanisms are still in place keeping the user safe.

So it's not as if somehow you install a piece of malware and, in general, all of a sudden all of your contacts are available or all of your data on your phone is suddenly available to the attacker.

Q. Does Android offer any sorts of security protections that are not on the phone itself?

A. Yes, it does.

Q. And what are those?

A. Well, if we look on the next slide, what I show off to the right is the review process that apps go through if they are submitted to the Play Store. So that's the first-party Google Store.

And so there are two components to that review process. The first is an automated review. So that's a review that is conducted by algorithms by these machine-learning pieces of software, and they're going to examine the app to look for signs of malicious behavior, you know, attempts to harm the users.

A subset of apps are also subject to a human review. So, for example, to maybe look for objectionable or obscene content or maybe to try to help the automated review out if the automated review couldn't issue a firm verdict about app maliciousness.

Q. Does Google's app review prevent all malicious apps from making its way onto the Google Play Store?

A. It does not, no.

Q. And are there any examples of apps that have made their way onto the Google Play Store that were malicious?

A. Yes. There have been various examples of this. There have been examples of sort of scam apps, for example, on the Play Store where you have apps that pretend to be a very well-known app, like Word or something like this, but actually are not that legitimate app; and as a result, users get tricked into installing that inappropriate app.

Q. So who is the reviewing entity for that review that you just described in the right-hand column here?

A. So the reviewing entity there is Google itself.

Q. And does an app that's reviewed by Google have to be distributed through the Google Play Store?

A. The answer is no. Because from a technical perspective, we can think about the reviewing process for an app as separate from the distribution process for an app.

Q. Are there third parties that can also conduct any sort of

app review?

A. Yes, third parties can do that and in many cases there are examples of that. So there are other app stores that conduct app review. There are also companies, like malware scanning companies, like Norton, for example, that also review apps for signs of maliciousness.

Q. Does Google do anything to review apps that are distributed outside of the Play Store?

A. It does. And so that's what I show kind of in that leftmost column that says "Off-Play App Review." And so at a high level, the review process there looks similar to the one that you see for Play Store apps. There is an automated review. There is also a human-driven review as well.

Q. Does Google dedicate the same resources to the off-Play review that it dedicates to the Play Store review?

A. It does not, and that's not just my opinion. There are in the production documents examples of Google's own security employees saying that off-Play app review has been underresourced to a pretty severe extent.

Q. So earlier, Professor Mickens, you said Google's machine-learning tools for detecting malware do not use installation source as an indication of maliciousness. What did you mean by that?

A. So by that I mean, think about what a machine-learning model does when it tries to determine whether an app is

malicious. That model is going to look at the app and try to -- and try to extract observations or characteristics. So it will look at the structure of the code. It might look at different types of data that the app contains, all these different sort of features.

And after looking at all those features, it will then say, "Well, do those features, you know, indicate that this app is going to be malicious?"

And so when I observed that Google's models don't look at the distribution channel as an important feature, that's important because it's saying that the models aren't really thinking that the distribution channel by which an app came from is a strong indicator of maliciousness.

And that makes sense; right? Because what does it mean for an app to hurt you? It means that it tries to steal your data or it tries to crash your phone. That's what it means for an app to be malicious, not what channel did it came from.

Q. So, Professor Mickens, I'd like to walk through some of the friction steps that you analyzeed for purposes of your opinion.

Could we start by taking a look at the friction steps involved in downloading something from the Galaxy Store? What would be the first --

THE COURT: Let me just point out, we have heard a lot about these steps. So let's focus on something knew and fresh.

How about that? Okay?

MR. CLARKE: So, Your Honor, in order to sort of expedite this, maybe I could just let Professor Mickens quickly walk through, and I'll follow along with the clicker so that we can get to kind of the comparison at the end, which I think is the salient point.

THE COURT: Okay.

Professor, we have heard a lot about the steps. So anything that's new, meaning not literally what you have to do, would be the best thing to do, and let's not dwell on it. If it's taking too long, I'll jump in. Okay? But you take it from here.

THE WITNESS: Okay. I'll try.

BY MR. CLARKE:

Q. So could you just quickly summarize for us the friction that's associated with a download from the Google Play Store?

A. Sure. So let's go to the next slide.

So in this case, the user is trying to install Wikipedia through the Play Store. There's an install button that they're going to see. They click on that install button.

Next slide.

And then they launch the app. So that's what happens in the Play Store.

Q. Okay. So it's a single-click installation process essentially; is that fair?

A. Essentially, that's right.

Q. Okay. So I'd like to turn to the process for third-party stores, and perhaps you could walk us through the first sort of four steps of that process.

A. Sure. So if we go to the next slide.

So we've already -- so what we can see here, even though it's grayed out, there's a lot more steps; right? And so what's the most salient thing with respect to this part of sort of my testimony?

Well, let's sort of click through. So we go to the next slide.

Okay. So here is a warning screen we didn't see before. And so that warning screen has some text there that, in theory at least, is trying to inform the user and allow them to make an important choice. And this is where I think sort of the novel part is that I want to try to tease out here.

Now, we saw from Mr. Kleidermacher last week a version of these videos. So it is -- it is true that the jury has seen these videos, but those videos are very -- they went -- he went through that process very quickly. Okay? And so an important aspect of security is users not only giving consent but giving informed consent.

So what I want to do very quickly is just walk through those warning screens and just make sure that the jury can understand what it would mean to give informed consent in this

case.

So, you know, for this screen right here, it says (as read):

"So for your security, your phone currently isn't allowed to install unknown apps from this source."

Okay. One thing I'll quickly flag here, calling Wikipedia unknown is a bit weird. Right? It's not clear that the user is actually being educated about the relevant security decision here by calling Wikipedia unknown.

Okay. So let's click through.

Okay. So now we see this install unknown apps setting screen here. So here, you know, what did the prompt say? Maybe you've seen this screen before, but let's see what the prompts say. So the prompt says (as read):

"Your phone and personal data are more vulnerable to attack by unknown apps."

Okay. Let me point out here that your phone is also vulnerable to attack by apps that are installed via the Play Store too. So this is not somehow a unique danger that this screen is talking about with respect to what can happen to you install when you apps. It can happen via third-party channels or first-party ones.

Q. Professor --

THE COURT: Can I just jump in?

So on that point, if you're downloading an app from the

Play Store, do you get this same warn?

THE WITNESS: No, you do not see this warning. In fact, we're using the same app both that initial Play Store walk-through we went through a couple seconds ago and here. So it's the same app. Its just Wikipedia. Right? So it's not like somehow the nature of its potential maliciousness has changed.

And, yet, here in this walk-through we're seeing this warning, and that's a problem. Right? And that's, in fact, a reason why it's important to look at these warning screens because we can tease out this dissonance in terms of, like, what Google is claiming these screens are doing for you, the user, versus what they're actually communicating to you.

BY MR. CLARKE:

Q. So one quick question on this screen.

Up until this point in the process, has the operating system actually looked at the identity of the app that's being downloaded to determine whether it's something that could potentially be risky?

A. No. And this sort of Plays off of the judge's question as well.

So all of this friction that's being imposed is based purely on the installation channel. Right? The fact that, like in this case, we're installing via the F-Droid third-party store.

THE COURT: If I may.

THE WITNESS: Please.

THE COURT: If it's on Play -- okay? -- if the app is on Play, has Google done any prescreening to vet it in a way that an unknown app would not have been prescreened for security?

THE WITNESS: So -- so it's a good question. So I think what we want to disentangle is the notion of reviewing from distribution.

So, for example, on the Play Store, all apps have to go through that review process. That's what I was kind of describing a couple slides earlier.

So if an app comes to the Play Store, it will have been reviewed. Now, what happens with, you know, other distribution channels? Let's say they're direct installation or a third-party app store in this case. It's entirely possible that the app has, in fact, been subject to a high-quality review.

In fact, like in this case, we're looking at the exact same app -- right? -- that the Play Store has reviewed and found it to be fine.

The problem is that right now, Android doesn't sort of reflect the fact that apps which come from non-Play Store channels may, in fact, have been subject to high-quality review.

And that's one of the key aspects of my expert opinion, which is that it's entirely possible that these non-Play Store distribution channels are distributing reviewed apps, but Android doesn't really have affordances that would sort of inform the user and make that clear to them. Instead, it's just putting up these friction screens about, you know, installation channels.

Thank you.

BY MR. CLARKE:

Q. Thank you, Professor.

Could you walk us through the rest of these steps in this friction flow?

A. Great. So if we just go to the next slide.

So let's assume that the user clicks over, gets to this next screen. And let me point out, by the way, it's not guaranteed that all users will even make it this far in the workflow -- right? -- because there's actually abandonment that may happen. Because users might get frustrated. They might say "I'm tired of having to click through all these screens." So it's a big assumption that the user's actually gotten to this point in the flow.

Anyway, let's assume they have. The user sees the screen "Do you want to install this app?" And let's assume that the user clicks "Yes."

And so here at this point, this is the first time in this

whole flow that Android has actually tried to look and see whether the app to install is actually malicious or not.

So what we're seeing here, you see how in 4B it says "GPP Prompt"? Okay? So "GPP" stands for Google Play Protect.

So once you've clicked, "Yes, I do want to install," now the malware scanner is going to run, and it's going to look and see if the app that you're trying to install is malicious.

Now, for the case of the Wikipedia app, the answer would be no. And so you would not see this friction screen I'm showing you here. I'm just showing you this just so you can kind of get an intuitive feel of what would happen if the app you were trying to install were malicious.

Q. So just to clarify, if the app was not flagged as malicious, would there be any kind of a warning screen or a warning prompt at this step?

A. There would not be. Similar to how like if you would install via Play, you know it's already been reviewed and you're not going to see like an extra screen there because it's been reviewed.

Q. Okay. So what happens for the rest of this download process?

A. Okay. So let's assume that the malware scan found no problems with the app to install.

So if we go to the next slide.

So the user is kind of presented back with this friction

screen we saw in step three. Let -- so now the user has to navigate out of that screen, so they click in the upper left-hand corner.

So if you go to the next slide.

And then, finally, the user can launch the app. And as I mentioned, there's going to be nontrivial abandonment through this process, so not all users are going to make it this far.

Q. Okay. Now, could we walk through, again expeditiously, how this process looks for a direct download?

A. Of course. So if we go to the next -- oh, here, we're already there. Sorry.

So now we're going to look at installation via direct installation, and in particular via a web browser. So we're going to download and install the exact same app that we were looking at before. Okay? So this is the Wikipedia app. So same app in all three cases.

So we go to the website. We find out where the app is. We click install.

Next slide.

Then we're going to see a warning saying "Do you want to download this app anyway?" To be clear, this is coming from the browser. Okay? So this is not coming from Android. It's not coming from the platform. This is a browser warning.

So let's click through.

The user sees the file download in that upper part of the

screen. The user clicks open. This is also a screen that's coming from the browser. It's not coming from the platform.

Next screen.

Okay. So now we see this sort of friction flow that we were examining before. Now, I've already read you these warnings here before, so I'm not going to do it again; but suffice it to say, that they are the same problems that we have here that we had with that other flow. Right? Why is it that Wikipedia is being claimed to be an unknown app? Why are we getting these complaints just because we're using a particular installation channel?

So if you click through to the next slide.

We've seen this screen before. There's a bunch of scary language here about your phone and personal data are more vulnerable to attack by unknown apps.

It's vulnerable from any app regardless of the distribution channel. And if you look at this sort of language at the end where it says that you agree that you are somehow responsible for any damage to your phone, is that -- I mean, Android has never presented you with some notion like a warranty that you're voiding if you are to install from this point, so this language is also not helping to inform users.

So let's assume the user hasn't abandoned the workflow.

Next slide.

You slide that slider over. Then we come to this confirm

installation prompt. Let's assume we click on that.

Here's where GPP runs again. Once again, the thing to call out here is that this is the first part of this entire workflow where the platform has actually tried to evaluate "Is this app actually malicious or not?"

All of this other stuff that you were seeing in terms of friction, it was based on what distribution channel are you trying to install the app through.

Q. Professor Mickens, one question, if I may.

Which of these steps that you just walked through so far would be most effective in protecting users from malware like FluBot?

A. So the step that would be the most effective in protecting users from malware is the step that we're looking at right now. That's the malware scanning step that is specifically looking at the app and trying to determine whether it's malicious or not.

Q. So there are a couple of steps above --

THE COURT: I'm just going to jump in.

So, okay, going to this GPP prompt that we're looking at here --

THE WITNESS: Yes.

THE COURT: -- you said this is the first time an actual security check happens; right?

THE WITNESS: Yes.

THE COURT: So could all those other steps that you've described as friction be skipped and could a user go directly from "I'd like to install this" to this GPP stage?

THE WITNESS: So I don't think they should be skipped; however, I think that those steps can be compressed, and I actually plan on addressing that exact point in a couple slides.

THE COURT: Okay. That's fine.

Go ahead.

MR. CLARKE: Thank you.

BY MR. CLARKE:

Q. So just the steps that are immediately above the GPP prompt, so the, for example, "Step 5: Allow install of unknown apps," how effective do you view that step as preventing installation of malware like FluBot?

A. It's a very, very crude hammer and I think a very ineffective hammer. So the FluBot that my counsel is referring to, that's something that Kleidermacher had brought up about being an app that's sort of distributed via direct installation. And he said that, you know, these types of friction screens help users because they will help them to abandon installs that may be risky.

Well, it's true that, you know, some users will abandon this workflow, let's say, when they're installing malware; and then, you know, a good thing would happen so the user wouldn't

install malware.

But in this case, this example I'm walking you through here, it's not malware that's being installed; its Wikipedia that's being installed. And so if you have people who drop out of that installation workflow, who abandon it because of that extra friction, that's a harm to users.

And it's a security problem too because it's not, you know, sort of giving users a calibrated understanding of what the risk is when they install apps from non-first-party sources.

Q. So, Professor Mickens, could you just sort of quickly walk us through the end of this download process?

A. Yes. So assuming that the GPP scan doesn't find any problems, the user clicks through -- or sorry -- doesn't click through. Excuse me. So there's no extra friction screen if there's no problems with the malware scan. So we go to the next step, and then we just launch the app.

Q. Thank you.

So, Professor Mickens, Mr. Pichai, Google's CEO, when he was here also testified, quote (as read):

> "We add steps just to make sure users are understanding their choice. You know, and friction sometimes in a security context is beneficial because you don't want to accidentally click on something which could completely compromise your phone."

Do you agree with that statement?

A. Well, I agree at a high level that friction when it is commensurate and proportional to risk is helpful for allowing users to make informed decisions. However, I do not think that the way that Android currently implements these friction screens are actually following this sort of security guidance that friction be commensurate and proportional with risk.

Q. What are the core decisions that users should be making with respect to installing apps on Android phones?

A. So I show those decisions on the next slide.

And, Your Honor, this is starting to speak directly to some of the questions that you were asking about what can be skipped, and so on and so forth.

So what I'm showing here are the two core decisions that require user consent during the process of installing an app.

So that first core decision is: Do I want to allow this app that I'm using as an installation mechanism, do I want to allow it to actually install things? So you can think of this as being like: Do I consent to this particular installer, the browser or, you know, a third-party store? Do I, as the user, feel comfortable allowing that installer to actually install things?

Q. And what's the second core choice?

A. The second core choice is that the user has to be able to ascertain: Well, has the app that I want to install, has it

been scanned? Has it been subject to a high-quality review for maliciousness?

And that's an important decision because, you know, the user, you know, most likely will not want to install an app that hasn't been reviewed or will at least want to be informed about that fact so that they can make their own decision, for example, based on their own research, about whether the developer of the app is reasonable.

Q. So, Professor Mickens, the steps that we just looked through a moment ago, at which point in that process does the user make the first decision that you described?

A. Right. So if we go to the next slide.

And so -- so, once again, Your Honor, now we're going to look more directly at the question that you were asking, so which steps can be removed or condensed, so on and so forth.

So the first security decision is: Does the user consent to allowing an installer to act as an installer?

Well, if we see in, let's say, the third-party store column, that's sort of the middle column, those sort of rows that are highlighted yellow there, at a high level what those rows are doing is they're asking that question that I just mentioned: Do I as the user want this particular installer to actually be able to install apps?

Now, what we see, though -- and this is why it was important for us to walk through that language -- is that the

security question being asked here is quite straightforward: Do I, as the user, want this app to act as an installer? But that clear, crisp language isn't described in those friction prompts, for example, those yellow ones that we see in that second column there.

And also there's multiple friction screens when really you only need one that directly addresses that question, and we see similar problems in the direct installation column as well.

Q. And so at what point in these processes does the user make the second decision that you described?

A. So recall that the second decision is: Can I, as the user, ascertain whether an app to install has been reviewed and, therefore, declared to be likely nonmalicious? That is being accomplished in those sort of purple GPP prompt steps that we see. So, like, 4B in the case of a third-party store and then 6B in the case of direct installation.

Q. And, Professor Mickens, what is your opinion of the friction that we are seeing on this screen here?

A. Well, this comes back to one of my core conclusions. I think that the friction that we're seeing in the second and third columns of this diagram, it's not proportionate to the risk, and the warnings that users are being shown are not informative with respect to helping them making an informed decision.

Q. Is there a way to empower users to answer those two core

questions with less friction on Android?

A. I think so. And so if we go to next slide, I can give you an example of what I call proportionate friction flow.

So reducing the number of friction screens while still allowing users to make informed decisions, an informed consent about app installation.

So here we're imagining a new world. Okay? So this is a proposal. This is not something that, you know, is out in the world right now. So let's imagine that we are installing an app via a third-party app store, and we're going to use Wikipedia app, once again. So we're keeping that app consistent in the examples.

So we go to this third-party store. There's that blue install button. The user clicks that.

So if we go to the next slide.

And so what we see here, let's assume that this is the first time that the user is installing via this third-party store. So in this case it's the F-Droid store. So in my proposed flow, my proposed friction flow, the user would see --

THE COURT: If I may jump in.

THE WITNESS: Yeah, go for it.

THE COURT: So the user is on a store called F-Droid. That's the app store?

THE WITNESS: Yes, Your Honor.

THE COURT: And they're downloading the Wikipedia app

from F-Droid?

THE WITNESS: Yes, Your Honor. That's right.

So the user decides to click "Install," and so now in this walk-through, we're assuming it's the first time that the user has installed via this third-party store, and you see the warning that we see here. So what does it say. It says "Allow Installation." That's sort of the title of the warning. And it says "Do you want F-Droid to be able to install other apps?" That directly answers the salient security question that users should be thinking about.

And now, finally, we've sort of gotten to the part where I directly address your question.

This is what I think those yellow rows that we were seeing before can be condensed to. This asks sort of the essence of the question. So that's what this screen is going to show.

BY MR. CLARKE:

Q. Okay. Any other steps in this process?

A. Yeah. So then let's say the user clicks on "Allow." So then at this point, there would be a verification of review. So that's basically just saying: At this point Android is going to ask "Has this app received a high-quality review? And if so, was it deemed to be safe by that review?" And so this is similar sort of to the GPP steps that we saw before.

If the app does not have a review, then the user will see this warning here which says "The app to install has not been

reviewed. Are you sure that you want to install it?"

Okay. Once again, the language here is very crisp, and it allows the user to give informed consent with respect to the decision to install a nonreviewed app.

Now, just as with the GPP step, if during this step Android determines that the app has been reviewed, you know, it has been marked as safe to install, you don't see this extra friction screen here. Okay? So this is only shown if the app hasn't been reviewed.

Q. Thank you.

And then what would the final steps here be?

A. So assuming that there's no problems with the malware scan, then the user will go to the next screen, and then they will just open the app.

Q. So how does this compare to the other friction steps that we looked at a minute ago?

A. Well, if we go to the next slide, this is sort of the comparison.

So in all of the three -- sorry -- in the second, third, and fourth columns, so in the third-party store installation, the direct installation and proportionate friction examples, that one off to the right, that's the hypothesized world I was talking about, we see that in all three of those cases there is a review that is sort of checked. In other words, like there will be a point where in all three cases Android is going to

say "Has this app been declared nonmalicious by a review process?"

The big difference is what we see with those yellow rows. Those are the rows that are asking that first security question: Do I, as the user, consent to allowing the installer to act as an installer? And so we see that -- once again, to the judge's question -- we've condensed those three screens, let's say, in the third-party store case, down to one screen. And we've actually tightened the language so that users can make that informed consent.

Q. And just to be clear, Professor Mickens, these are first-time installation friction flows just so that it's --

A. That is correct. That is correct.

And so after, for example, a user has consented to allowing an installer to act as an installer, the user is not going to continually get prompted to allow that installation to take place.

Q. And that's true for each of these columns; is that correct?

A. Yes, sir.

Q. Okay. Thank you.

So in a world with proportionate friction, which of these steps that are appearing in the second and third column would fall away?

A. So in the second and third column, basically -- so let's

look at the second column, for example. So in the second column showing the third-party app store workflow, if you look at steps two, three, and five, so "Proceed to settings," "Allow unknown apps," "Navigate out of settings," those would all be sort of condensed to a single permission prompt, which is essentially: Do you want to allow this installer to act as an installer?

Q. Professor Mickens, why don't we see any highlighting in the left-hand column here?

A. The reason that you don't see any highlighting in the left-hand column, it's twofold. So, first of all, there's no verify review row because for apps that are coming to the Play Store, the sort of Play Store app on the user's phone knows that those apps have already been reviewed, so it doesn't have to do an explicit step there.

And the reason why you don't see the yellow highlighting is that basically the Play Store is assuming that the user has already consented to allowing the Play Store to act as an installer.

Q. So in the far right-hand column, your proportionate friction column -- do you see that?

A. Yes.

Q. -- there's a step that says "2B, Verify Review"?

A. Yes.

Q. Could you explain what you have in mind with verify

review?

A. Sure. So that's the part where the platform is going to determine whether the app to install is actually malicious or not, and so it will do that by trying to see if the app has been reviewed by a high-quality review service.

Q. And who actually is going to review those apps in the scenario that you have in mind?

A. So it could be Google. It could also be Google plus certified third parties.

Q. Does an app have to be reviewed by the same entity that's distributing the app?

A. It does not, and this gets back to a point I made earlier about the review process for an app. That can be decoupled from the distribution process for an app; in other words, how it gets onto users phones.

Q. So how could Google review apps that are being distributed outside of the Google Play Store?

A. Well, I show how that might take place on the next slide.

So here we're going to examine a proposal that I call centralized notarization. You can think of notarization as just being shorthand for trying to determine whether an app bears a stamp of approval, whether it's been notarized by a reviewing entity and declared to be safe by that reviewing entity.

So in this proposed world, you've got the developer who

works on an app, and then that developer is going to submit -- next slide -- the app to Google for review. And then assuming that the app is reviewed successfully, then Google is going to return back a notarized version of the app.

And so I show that little checkmark there. That's sort of the notarization seal of approval. That's basically sort of a cryptographically signed statement that says Google has reviewed this app and found it to be nonmalicious.

Q. And what happens next in this process?

A. And so next what will happen is that the developer can actually distribute this app through whatever channel a developer pleases.

And so if we go to next slide, we see that the developer might actually distribute the app through the Play Store; the developer might also/or distribute the app through a third-party app store; or make it available through direct installation, for example, via web browser.

And note that in all three cases, the app that the developer distributes bears that notarization seal, that sort of signed statement that indicates that Google has found the app to be nonmalicious.

Q. And what's the next step in this process?

A. So then the next step is just that the user locates the app in some way and then tries to install it. And then at the point of installation, this is where we see that 2B step, the

verify review.

So we can see up on the slide it says that Android confirms the signature at the point of installation. That means that Android is going to check to see if the app bears that notarization sort of stamp of approval. If so, Android does not show that friction screen that I mentioned before that says, "Hey, this app has not been reviewed. Are you sure that you want to install it?" But if the app has been reviewed, then you won't see that friction step in 2B.

Q. Are there any companies out there that use a model like this?

A. Yes. So at a high level, if you look at Mac OS, Mac OS has this notion of notarization as well. So as some you may know, on a Mac OS machine there's a first-party Mac OS store, but there's also this ability for a developer who doesn't want to distribute through that first-party store to instead just submit the app to Apple. Apple will scan that app looking for malware; and if no malware is found, essentially the app will get a notarization stamp of approval just like we have here.

Q. And how difficult would it be to modify Android to support this sort of an approach?

A. Not difficult, and the reason is because most of the machinery that you would need inside of Android to make this work, so, for example, the checking of signatures, that's already there in the code. So you wouldn't have to reimplement

a lot of stuff.

Q. So if Google didn't want to review all of these apps itself, are there any other alternative models that it might be able to adopt?

A. Yes. So I've thought about a proposal for that as well, and I've called it decentralized notarization.

So if we can go to the next slide.

And so what do we see here? Well, this workflow looks a lot like the centralized notarization workflow that we saw earlier. The only real difference is what we see sort of in the bottom left-hand side of the slide.

So the developer has their app. They upload it to a reviewing entity. Now the reviewing entity might be Google, but it might be some third-party reviewing entity that Google has certified as being, you know, capable of providing high-quality reviews.

So the developer submits their app to one of these reviewing entities. If the review succeeds, the notarized version comes back, and then the workflow looks exactly like it looks before. So the developer can distribute their app through whatever distribution channel they want. The user finds it. And then at the time of installation, Android is going to look to confirm the signature, to confirm whether or not that review has actually been performed for that app.

Q. So were you present when Mr. Kleidermacher testified last

week?

A. I was.

Q. And did he provide any testimony that changed your opinion on this topic in any way?

A. No, he did not. And, in fact, he talked about this group called the App Defense Alliance, which is a group of third-party security companies that Google is already working with to try to analyze various aspects of app security. So I think this proposal is quite imminently implementable.

Q. Did you hear Mr. Kleidermacher testify that Google can't make the Internet safe?

A. I did hear that testimony, yes.

Q. Would your proposals require Google to police the entire Internet?

A. They would not. And so if you look at this workflow, Google is -- sorry. Let me back up a little bit.

In the centralized proposal for notarization, Google is only responsible for reviewing those apps which were submitted to it directly. Not all developers are required to do so, and Google wouldn't have an obligation to look at them.

In the decentralized approach, if Google for whatever reason were worried about scaling up that reviewing load, well, here we've got a bunch of third parties that can help shoulder some of that reviewing load for Google.

Q. And are there any other platforms out there that use sort

of a decentralized security verification scheme?

A. There are. And perhaps the most sort of well-known example of this is the web.

So if we go to the next slide.

So if you go to the web and, once again, you go to one of these https sites, so what is the S giving you? Among other things, it's giving you, the user, sort of a guarantee that the site that you're talking to is actually run by whoever you think that the owner of the site should be.

So if you go to apple.com, that little lock icon that we see in the bottom right, that's saying that an identity verifier has guaranteed that this web server is actually owned and operated by Apple and can speak with the authority of Apple.

And so who performs this type of identity verification for websites? Like on the current web, it's not the future web, the current web. Well, already if you look at the browsers that are made by popular vendors -- like Google Chrome, for example, like Microsoft Edge -- they already trust a decentralized set of identity verifiers for the web. So Google is an example of one of those. So is Verisign. So is GoDaddy, so on and so forth.

So this decentralized way of verifying identities, this underlies the security of the web. And Google already trusts it because they made a browser which trusts it, and they run a

bunch of web properties, web services, like Gmail, that rely on the safety of https and decentralized verification.

Q. So, Professor Mickens, would any of these proposals that you're outlining undermine the device level security of Android phones?

A. They would not. None of the proposals that I mentioned touch those device-level security mechanisms at all. So the OS still provides, for example, all those security mechanisms I mentioned earlier.

Q. If Google were to adopt any of these proposals, would it make Android less secure for users?

A. No. And, in fact, it might actually make Android more secure. Because let's think about the two separate proposals I've made for centralized versus decentralized notarization.

In the centralized approach, who is the entity that's doing all of the reviews? It's Google; right? And so Google still gets to set all of those review standards.

Now, in the decentralized world, it's possible that there are these third parties who would also perform reviews in addition to Google; but, importantly, Google is the one who's certifying those third parties. Google is setting the minimum quality bar for those reviews.

And so at worst, security would stay the same, but it's also possible that some of those third-party reviewing entities would do a better job than Google and actually keep users more

safe.

Q. Thank you.

MR. CLARKE: Your Honor, I pass the witness.

THE COURT: Okay. Let's take our lunch break. I have something I have to attend to at 12:15. So we'll come back at 12:40. Okay? A little extra lunch.

Okay. So I'll see you at 12:40.

(Luncheon recess was taken at 11:58 a.m.)

AFTERNOON SESSION **12:46 p.m.**

(Proceedings were heard out of the presence of the jury:)

THE COURT: Who do we have after this witness?

THE CLERK: All rise.

(Proceedings were heard in the presence of the jury:)

MR. BORNSTEIN: Next, Your Honor?

THE COURT: Yeah, who's next?

MR. BORNSTEIN: We're doing back to back. So we'll have a security expert from Google.

THE COURT: Oh, okay.

Okay. Please, go ahead.

MR. OLASA: Good afternoon, Your Honor. Kuru Olasa for Google.

CROSS-EXAMINATION

BY MR. OLASA:

Q. Good afternoon, Professor Mickens.

A. Good afternoon.

Q. So, Professor Mickens, let's start with your Demonstrative 44.

Can we have that put on the screen?

Now, the left hand of this slide, the left-hand column, shows the installation from the Google Play Store; is that right?

A. That's correct.

Q. And all apps on the Google Play Store have been reviewed by Google; right?

A. That's correct.

Q. Okay. And looking all the way over to the right, that's one of your proposals in this case, the proportionate friction proposal for third-party stores; right?

A. That's correct.

Q. And in that rightmost column, there's a step click, install; another step grant, install permissions; and then a step called 2B, verify review; correct?

A. Correct.

Q. And the verify review step is where a check will be done to see whether the app had been reviewed; is that right?

A. That's correct.

Q. And you have two proposals in this case to verify whether an app had actually received any review; correct?

A. I believe you're referring to the centralized and decentralized notarization proposals.

Q. That's right. And those are your two proposals in this case; right?

A. That's correct.

Q. Okay. So let's talk about those two proposals, and begin with centralized notarization.

And can we put Demonstrative 20 up, please?

So with centralized notarization, Google would become the only entity that the Android operating system trusts to review apps; correct?

A. I wouldn't say become. I mean, it would be similar to the status quo that you have now on Android.

Q. Well, Google would be the only entity that Android would look to to determine whether an app had been reviewed; right?

A. That's correct.

Q. Okay. And under this proposal, Google would carry the entire burden for reviewing all apps on Android; right?

A. Well, it would bear the entire burden in terms of performing the reviews that the Android OS would sort of know or the ones to look for at app installation time.

Q. Right. And so Google would be the only entity that reviews apps and would have the entire burden for reviewing all apps on Android; correct?

A. No. So there could be other entities that could review apps on Android; but purely with respect to what reviewing entities would Android be aware of, Google would bear that

burden.

MR. OLASA: Your Honor, may I put up a portion of the expert report? This is Tab 2, page 115, paragraph 253.

THE COURT: 253?

MR. OLASA: Paragraph 253 on page 115 of Tab 2.

THE COURT: Just the first sentence?

MR. OLASA: Can we put it up?

THE COURT: Just the first sentence?

MR. OLASA: Just the first sentence, yeah.

THE COURT: You can do the second sentence up to "tokens" comma.

MR. OLASA: Tokens comma. Thank you, Your Honor.

Mr. Nickels, can we put up the sentence beginning "I describe" until "tokens" comma?

BY MR. OLASA:

Q. This is an excerpt from your expert report; right, Professor Mickens?

A. That's correct.

Q. And you signed this expert report; correct?

A. I did.

Q. And you believe everything in this expert report was accurate; correct?

A. I do.

Q. And you wrote in this expert report that under your centralized notarization proposal, Google carries the entire

burden for reviewing apps; correct?

A. For the apps that will be receiving that low-friction experience on Android, yes.

Q. Okay. So let's break down how this would work.

If an app passes Google's review under your proposal, it will get a special token; correct?

A. Yes.

Q. And the operating system will then check for that token when the user tries to install the app; right?

A. Correct.

Q. And if the app has a token, then it won't get any warning under your proposal; correct?

A. It would not receive the, you know, "Warning: You're about to install an unreviewed app."

Q. And you call that a low-friction installation experience; right?

A. It is low friction compared to the current workflows, yes.

Q. But if the app doesn't have a token, it would still get a warning; correct?

A. Correct.

Q. If an app hadn't been reviewed by Google, there would still be warnings; right?

A. Correct.

Q. Okay. Now, under your proposal, Google will be the only entity that can hand out these tokens; right?

A. In the centralized approach, yes.

Q. Right. We're talking about your centralized approach now; right?

So under your centralized approach, Google is the only entity that can hand anyone these tokens; right?

A. Correct.

Q. No one else can hand out the tokens, just to be clear; right?

A. In the centralized approach, correct.

Q. And the only way an app developer can get a token would be to submit their app to Google for a prepublication review; right?

A. That is correct.

Q. And Google would set all the standards for this review; right?

A. Correct.

Q. Okay. And your proposal in effect would actually hand Google a lot more authority over app review; right?

A. I don't believe that's true.

Q. All right. Let's walk through how this would work.

So you understand that on a Samsung Galaxy -- on a Samsung phone, the Samsung Galaxy Store comes preinstalled; right?

A. That's often the case, yes.

Q. Right. And in a world without your proposal, an app installed from the Samsung Galaxy Store on a Samsung phone

won't get the warnings we were talking about earlier; right?

A. If it's preinstalled, that's correct.

Q. Okay. It would give a low-friction install experience; right?

A. If it's preinstalled, yes.

Q. Right. And so let's use another example. Epic Games, they make the Epic Games Launcher; right?

A. Correct.

Q. And that's an app that you can then download Epic's Fortnite app and Epic's other games; right?

A. Correct.

Q. And in today's world, if the Epic Games Launcher is installed from a Samsung Galaxy Store, it won't get any warnings; right?

A. That is accurate, yes.

Q. They'd get this low-friction experience that you described; correct?

A. It won't receive any warnings, yes.

Q. And that's regardless whether Google has or has not reviewed the Epic Games Launcher; right?

A. That is correct.

Q. All right. But in your proposal, Epic would need to come to Google and get a token in order to get this low-friction install experience; right?

A. That's correct.

Q. And that's true even on a Samsung Galaxy phone; correct?

A. Correct.

Q. All right. So let's put that point on the screen.

And the next one too. Sorry.

And, in fact, in 2018, Epic actually put its Epic Games Launcher in the Samsung Galaxy Store; right?

A. Yes.

Q. And it didn't have to submit that app to Google for review; right?

A. That is correct.

Q. And Epic, in fact, did get this low-friction install experience from Samsung; right?

A. Correct.

Q. And to this day, Epic still gets that low-friction experience?

A. Yes.

Q. But under your proposal, under your centralized notarization proposal, Epic would have had to submit its app to Google to get a low-friction experience; right?

A. That is correct. To get that malware review, yes.

Q. Right. And in today's world, preinstalled stores, like the Samsung Galaxy Store, they can choose to give companies like Epic a low-friction install experience on their devices; right?

A. They can choose to.

Q. Right. Now, you didn't check with Samsung about this centralized notarization proposal; right?
A. No, although such checking wouldn't be necessary to make the proposal.
Q. Right. In fact, you didn't check with any OEM about it; right?
A. No, but that's not necessary to evaluate its feasibility.
Q. Right. And you didn't ask any OEM if they would be willing to accept this change to the way Android works; right?
A. I didn't do that type of survey, no.
Q. And you have no proof either way as to whether an OEM like Samsung would be willing to accept this change; right?
A. I think it's reasonable that they would, but I don't have proof that they would.
Q. And you actually can't predict whether an OEM would demand financial payment from Google to agree to your proposal; right?
A. They may or may not.
Q. And you don't know one way or the other; right?
A. I can't predict the future with perfect clarity, no.
Q. And you didn't analyze that in your report; correct?
A. No, but that wasn't a relevant thing to do, to evaluate the reasonableness of the proposals from the security perspective.
Q. And, in fact, your reports in this case, they don't address at all whether OEMs would push back on your proposal;

right?

A. Well, the proposals were evaluated with respect to whether they would impose any undue burdens technically on OEMs or other people on the Android ecosystem.

Q. Professor Mickens, that wasn't my question. My question was pretty specific.

Do your reports in this case address whether OEMs would push back on your proposal?

A. So the proposals are designed in a way that I don't think such pushback would be likely. So, yes, in a sense, I have considered that, but there is no line in the report which says, you know, "Section 8B, Pushback."

Q. Your report does not explicitly address the issue of OEM pushback; correct?

A. Not explicitly, no.

Q. Now, you also didn't put a dollar amount on how much it would cost for Google to implement centralized notarization; right?

A. Correct.

Q. And you can't tell the jury, therefore, how much it would cost Google; right?

A. I can talk about it in scalability terms, but I can't talk about it in terms of a raw dollar amount.

Q. And, in fact, your centralized notarization approach would require Google to scale up its Cloud infrastructure to handle a

larger volume of reviewing requests; right?

A. That's a possibility, yes.

Q. And that's a possibility you outlined in your report; correct?

A. Yes. It might also reduce Google's burden.

Q. In your report you explained that the centralized approach would require Google to scale up its Cloud infrastructure; correct?

A. That's true in some cases, but the reply report actually provides some more commentary on that.

Q. And your centralized approach would also require Google to scale up its human review teams; correct?

A. That's a possible outcome, but it also might go down.

Q. And you don't say how much it would cost to scale up Google's human review teams for this centralized approach; correct?

A. I only talk about it in scalability terms.

Q. And you don't put a dollar amount on it; correct?

A. I don't put a dollar amount on it.

Q. Let's add that to the screen.

Now, you didn't express any opinion on how much Google should charge developers for this centralized notarization app review; right?

A. I didn't make any commentary about that.

Q. Right. You didn't say how much a developer should have to

pay to go through this app review process that you propose; right?

A. That's correct.

Q. In fact, in your proposal, Google could charge for a review if it chose to; correct?

A. Yeah, my report didn't talk to that.

Q. Right. In your proposal, Google could choose to charge for app review based on an app's size; correct?

A. It could. That's a thing that could happen.

Q. It could happen; right?

A. There's nothing that technically prevents that type of thing from taking place.

Q. And, similarly, under your proposal, Google could even charge a developer a percentage of the revenue earned by the app; right?

A. That's a thing that could happen from the technical perspective, yes.

Q. Right. So let's add that to the screen.

So I just want to make sure I have this right. Under your proposal, Google would carry the entire burden for Android app review. There would be a warning screen for any app that was not submitted to Google. You don't know whether OEMs would agree, you don't know the cost to Google, and you don't know the cost to developers; is that right?

A. I would not agree with that characterization.

Q. Well, one more thing about centralized notarization, Professor Mickens.

It isn't consistent with the Android platform security model document you showed earlier; correct?

A. How do you mean?

Q. Well, is it consistent?

A. What is "it"? Sorry.

Q. Your centralized notarization proposal.

A. I believe that it is consistent with that.

Q. Let's take a look at one of your slides.

Can we put up Professor Mickens' Slide 16, please?

So this is the Android platform security model paper you relied on; right?

A. That is correct.

Q. And you wrote -- and you focused on this open-ecosystem access point that's shown in the black text; right?

A. Correct.

Q. And in the gray text, there's further text that says "Central vetting of developers or registration of users is not required"; correct?

A. I see that text, yes.

Q. That's part of the Android security model; correct?

A. Yes, that's right.

Q. Okay. And there's more to the Android security model. Could you take a look at Exhibit 11105 in the binder in front

of you?

MR. OLASA: Your Honor, may I publish 11105 on the screen?

THE COURT: Why don't you ask the witness what it is first.

MR. OLASA: Sure. I'll lay some foundation, Your Honor.

BY MR. OLASA:

Q. Is Exhibit 11105 the Android platform security model paper you relied on and that we looked at a moment ago?

A. It is.

Q. All right. And --

THE COURT: Is there any objection to this?

MR. OLASA: I'm not offering it, Your Honor. I'm just going to cross-examine the witness on it.

THE COURT: Is there any objection to showing this?

MR. CLARKE: I have no objection to showing it, Your Honor.

THE COURT: Okay. This is not in evidence.

MR. OLASA: I'm not offering it, Your Honor. I just want to ask the witness some questions about it.

THE COURT: Don't just put chunks of it up. Ask questions; and if you want to impeach him, do it that way.

MR. OLASA: Absolutely.

\\\

BY MR. OLASA:

Q. Could you turn to page 5 of Exhibit 11105?

A. Okay.

Q. Do you see the paragraph in the middle that starts with "Untrusted code is executed on the device"?

A. I do see that paragraph.

Q. And that paragraph goes on to say (as read):

"One fundamental difference to other mobile operating systems is that Android intentionally allows, with explicit consent by end users, installation of application code from arbitrary sources and does not enforce vetting of apps by a central instance."

Do you see that?

A. I see that text, yes.

Q. And that is part of this Android platform security model paper; correct?

A. And something that my proposals still allow.

Q. Under the Android platform security model, Android does not enforce vetting of apps by a central instance; correct?

A. That's correct, and nor does my proposals for notarization.

Q. Let's talk about your other proposal, decentralized notarization.

And can we put on Professor Mickens' Demonstrative 47, please?

Now, decentralized notarization is similar to your centralized notarization proposal except that the tokens we were talking about could be provided by multiple reviewing entities, not just Google; right?

A. That's correct.

Q. But Google would be in charge of setting the standards for who qualifies as one of these third-party reviewing entities you show at the bottom of the slide; correct?

A. Right. So Google would serve as a certification authority determining which companies meet Google's security bar.

Q. And you don't actually have a specific proposal for what standards Google should apply; right?

A. Well, I mean, they could be similar to the ones that Google uses currently with the App Defense Alliance, for example.

Q. I understand. But do you have any specific proposals for what standards Google should apply in certifying these third-party entities?

A. Well, Google gets to set those standards. That's true in the centralized and decentralized case.

Q. So Google could pick the standards; is that right?

A. That's right.

Q. And then all of those reviewing entities would then have to apply Google standards; right?

A. They have to what?

Q. Apply Google standards; right?

A. Yes. So their review processes would have to meet that sort of quality bar that Google set.

Q. And Google would have to review and audit these third parties to make sure that they were meeting those standards; right?

A. Yeah, similar to what happens today in the browser CA infrastructure, that's right.

Q. And, again, you haven't checked with any OEM as to whether they would accept this decentralized notarization proposal; right?

A. By "OEM" you mean like a phone OEM?

Q. Any OEM. Like Samsung.

A. I have not checked with OEMs, no.

Q. So a moment ago you drew an analogy to browser certificate authorities, and you did that in your direct testimony as well. Do you recall that?

A. I do.

Q. Now, browser certificate authorities, they issue web certificates; right?

A. That's correct.

Q. And a web certificate doesn't mean that a particular website is safe; right?

A. Well, it indicates certain things about the security properties of that website.

Q. Well, a web certificate authority doesn't review whether a website is hosting malware; right?

A. That's correct.

Q. And a web certificate authority isn't even required to review the website's content in any way; right?

A. That's correct.

Q. And your reports don't identify any modern operating system that has implemented decentralized notarization for app review; right?

A. That is correct.

Q. You haven't identified a single modern operating system that implements this proposal; right?

A. Not my exact proposal, but it's similar to other types of technologies that are out in the wild today.

Q. In fact, you agree that no popular consumer operating system has ever implemented decentralize notarization for app review; right?

A. True, but looking at what is and saying --

Q. Is that right, Professor Mickens? Is that correct?

A. Correct.

Q. And that's because applying decentralized notarization to app review would be a new domain; correct?

A. What do you mean by "new domain"?

Q. Have you used those words to describe the application of decentralized notarization to app review?

A. I mean, it would be a new domain in the sense of there would be infrastructure that we'd have to build that doesn't currently exist.

Q. And you're proposing that Google should enter this new domain; right?

A. I'm proposing that it is a thing that they could do, and it wouldn't have that much cost in terms of additional resources.

Q. Now, Epic -- Epic Games, the plaintiff in this case, they haven't entered this new domain; right?

A. By "new domain" are you talking about my proposed notarization schemes?

Q. Let me break it down.

Epic Games operates a game storefront on PCs; right?

A. That's right.

Q. And users can go to that storefront and they can download games; right?

A. That's right.

Q. Epic Games does not trust third-party entities to certify the games on its store; right?

A. Not to my knowledge.

Q. Epic trusts only Epic; right?

A. To my knowledge, yes.

Q. Professor Mickens, Epic is paying you for your work on this case; correct?

A. That is correct.
Q. And you are paid about $750 an hour; is that right?
A. That's right.
Q. How much in total have you earned for this engagement?
A. I think roughly $150,000.
Q. All right. Let's turn to sideloading.
So would you agree, Professor Mickens, that the computer security community recognizes that sideloading on mobile devices is risky for the average user?
A. I think it's more subtle than that, the security community's stance on sideloading.
Q. You think many people in the security community recognize that sideloading on mobile devices is risky for the average user?
A. I think that there are a variety of opinions on sideloading.
Q. All right. Are you familiar with the Cybersecurity and Infrastructure Security Agency?
A. Yes, I am.
Q. That's a federal agency; right?
A. Yes, that's right.
Q. And it goes by the acronyms CISA or CISA?
A. That's correct.
Q. And CISA hires experts in computer security; right?
A. They do.

Q. And you're aware that CISA offers guidance on computer security issues; right?

A. I am aware of that.

Q. And CISA's guidance on sideloading in particular was brought to your attention by Professor Qian, Google's expert in this case; right?

A. Correct.

Q. All right. So could you turn to Exhibit 6595 in the binder in front of you?

A. (Witness examines document.) Got it.

Q. And Exhibit 6595 is guidance from CISA; correct?

A. That is correct.

Q. And it's on privacy and mobile device apps; right?

A. That is correct.

Q. And there's a heading on the first page "How can you avoid malicious apps and limit the information apps collect about you?" Do you see that?

A. I do see that.

Q. And below that there's a sentence that says (as read):

"Reduce the risk of downloading PHAs by limiting your download sources to official app stores, such as your device's manufacturer or operating system app store."

Do you see that?

A. Yes.

Q. And that was the advice given by CISA; right?

A. Well, there's also that second sentence, which says (as read):

"Additionally, because malicious apps have been known to slip through the security of even reputable app stores, always read the reviews and research the developer before downloading and installing the app."

So that advice is more subtle than I think you would find here.

Q. I understand. But CISA advises users to limit their risk of downloading potentially harmful apps by limiting their downloads to official app sources -- app stores; correct?

A. That's part of the guidance.

Q. And CISA also says immediately after that sentence (as read):

"Do not download from unknown sources."

Correct?

A. It says that, yes.

Q. And this was guidance that, again, Professor Qian brought to your attention in his report; right?

A. That's correct.

Q. And you submitted a reply report after that; correct?

A. I did.

Q. And you don't mention this guidance in your reply report; correct?

A. I do not.

Q. And Professor Qian brought guidance to your attention from many government agencies and third parties; right?

A. That's correct.

Q. And your report doesn't mention any of those examples; correct?

A. That's correct.

Q. Now, do you agree that sideloading can result in malware infections?

A. It is one way that malware can arrive on a user's device.

Q. And a sideloaded app may not have been reviewed for malware?

A. May or may not have been.

Q. Right. All apps on Google Play are reviewed for malware; right?

A. Correct.

Q. But a sideloaded app may or may not have been reviewed for malware?

A. Correct.

Q. And would you agree that an app that has been reviewed for malware is safer to install than one that hasn't received such a review?

A. More likely to be safe, yes.

Q. Now, in your report you visited a website called APKFab to test direct downloading from that website; right?

A. Yes.

Q. All right. So let's -- so this weekend, you know, I visited APKFab and searched for Netflix. So I'm going to put a demonstrative up to talk to you about.

Could we put up Demonstrative 2?

So I visited APKFab and I searched for Netflix, and here are the results I got.

Do you know if Netflix actually distributes its app through APKFab?

A. I'm not sure.

Q. Do you think it's likely?

A. It's possible.

Q. Do you think it's likely?

A. I don't know. I'd have to do some more research into it. I don't know.

Q. You have no idea one way or the other whether it's likely that Netflix actually officially distributes its app through APKFab?

A. In the same way that if I search on the Play Store and see a bunch of copycat apps, I'm not sure which one is real or if the developer actually distributes through there.

Q. Let's take a look at one example of the apps here. I'm going to point you to the second icon on the leftmost row and click on that one, and see what it shows us.

So that's the app I saw, and there's a little green icon that says "Trusted app." Do you see that?

A. I do.
Q. APKFab appears to be saying that this app is a trusted app; right?
A. Correct.
Q. What does APKFab do to review this app?
A. So I'm not aware of the detailed process that APKFab uses.
Q. You have no idea if APKFab does any review at all of this app; right?
A. I'm not sure.
Q. For all you know, that trusted app badge is given to every app; right?
A. I don't think it's given to every app, but I don't know what the detailed review process is, no.
Q. Do you know one way or the other whether that badge is shown for every app on APKFab?
A. I don't believe that it is, no.
Q. And either way, you don't know how that badge was put on the app; right?
A. That's correct.
Q. Do you know who runs APKFab?
A. I don't know what company runs it, no.
Q. You have no idea; right?
A. I don't know.
Q. Now, the page for this app shows Netflix screenshots. Do you see that?

A. I do.

Q. But the actual packaging for this app appears to be something called com.tveeemobilee.nitflix. Do you see that?

A. I do.

Q. This isn't the real Netflix app; right?

A. I would imagine it's not.

Q. This is probably malware of some type; right?

A. I don't know if it's malware, but it's most likely not the legitimate Netflix app.

Q. And you know that malware often pretends to be a popular brand; right?

A. It appears to be a popular --

Q. It masquerades as a popular brand; right?

A. That happens, yes.

Q. All right. You testified earlier, Professor Mickens, that the operating system can provide protections to users from malware; right?

A. Correct.

Q. But the operating system can't protect a mobile device against all malware attacks; right?

A. I agree.

Q. There's some types of malware that an operating system just can't stop on its own; correct?

A. Correct.

Q. And you also talked about some defenses built into the

operating system, like sandbox. Do you -- sandboxing. Do you remember that?

A. I do.

Q. And despite these defenses, the operating system can't stop all malware on its own; right?

A. Correct.

Q. For example, users could allow an app outside its sandbox; right?

A. Excuse me. What do you mean?

Q. A user could ask -- could give an app permission to escape its sandbox; right?

A. A user can grant permissions to an app to, you know, access devices or things like that.

Q. And one of those permissions could be to allow an app to access data from another app; right?

A. Not quite. So there are permissions that allow an app to access more data than would be in its private sandbox, but there are no permissions, to my understanding, that would allow it to access all data on the phone.

Q. Are you familiar with the accessibility permissions on an Android device?

A. I've heard of those, yes.

Q. Do you know if the accessibility permissions on an Android device allow an app to access data from another app?

A. So my understanding of those permissions is that they

allow an app to do things like display screens like over other apps, and things like this. It doesn't provide a total sandbox jailbreak, though.

Q. In any event, despite those protections we were discussing earlier, the operating system just can't stop all malware on its own; right?

A. On its own, that's correct.

Q. Now, you've heard the term "Defense in Depth" as applied to computer security; correct?

A. I have.

Q. In fact, you teach this concept in your classes?

A. I do.

Q. And the idea behind Defense in Depth is that an attacker's job becomes much more difficult when a device has multiple layers of defense; right?

A. That's the idea, yes.

Q. And there's wide agreement in your field that systems should be designed with Defense in Depth in mind; right?

A. That's right. Nothing about my proposals are opposed to that principle.

Q. Right. And you agree that it's a bad idea to rely on just one layer of security to protect users; right?

A. Correct. I believe in the principle of Defense in Depth.

Q. Right. And you believe the operating system shouldn't be the only layer of security; right?

A. Correct, but I believe this it is the most fundamental one. It enables other types of Defense in Depth.

Q. But it shouldn't be the only one; right?

A. Correct.

Q. All right. So let's talk about the sideloading consent screens.

MR. OLASA: And, Your Honor, I'll make sure we don't go through them in great detail. I understand the instruction.

So I first want to put up a demonstrative, Demonstrative 6, Mr. Nicols.

BY MR. OLASA:

Q. Is Demonstrative 6 based -- or a reproduction of something out of your expert report, Figure 24?

A. Yes, I believe it is.

Q. And that was an actual test you and your staff ran; correct?

A. That's correct.

Q. On an actual Android device; right?

A. That's correct.

Q. And you put it in your report because you thought it was a fair representation of the sideloading process; right?

A. That's right.

Q. Okay. So there aren't 16 or 19 steps to sideload shown here; right?

A. In this particular diagram, no.

Q. And when you tested this out, you were able to sideload an app from a website with just these steps; right?
A. That's correct.
Q. And some of these steps aren't consent screens or warning screens at all; right?
A. No. I think that with the exception of Step 6, these are consent or warning screens.
Q. So Step 1, navigate to the APK pure website, that's a consent or warning screen?
A. So, no, that was not a consent screen.
Q. So some of these steps are not consent or warning screens; right?
A. Some of them, yes.
Q. And some of these steps you actually think are reasonable; right?
A. Well, I think that at a high level, to the extent that these screens reflect the two security questions that I mentioned, they are reasonable, but the implementation of these friction screens is not reasonable.
Q. Okay. So let's drill down on that, and we'll make it quick.

So the first step you said that's just the user going to the website and clicking somewhere to download an app; right?
A. That's correct.
Q. Not a warning or consent screen; right?

A. That's correct.

Q. All right. So we can drop that one.

Let's go on to the next slide.

All right. Step 2, you testified that's a browser warning; right?

A. Step 2, that's correct.

Q. And the browser warning is something shown by a web browser, not the operating system; right?

A. Accurate.

Q. You heard Mr. Kleidermacher say that in his testimony; right?

A. I did.

Q. Yeah. And you agree that that's not part of what the operating system is doing?

A. Correct.

Q. All right. So let's drop Step 2.

All right. So can we go on to the next slide?

Okay. So we'll come back to Steps 3 and 4, but really quick, I want to get your opinion on Step 5.

Step 5 here is the user confirming an app install; right?

A. That's correct.

Q. And you think Step 5 is reasonable; right?

A. Yes. Users should have to give consent to installing an app.

Q. Right. Before an app is installed, a user should have to

consent to that; right?

A. That's right.

Q. So let's drop Step 5.

I think you told me earlier that Step 6 is not actually friction. It's a shortcut to open the app; right?

A. Correct.

Q. Right. So it's not -- it's not an additional step the user has to navigate to install an app; correct?

A. Correct.

Q. All right. So let's drop Step 6 from this.

So that leaves us with Steps 3 and 4. Now, Steps 3 and 4 require the user to consent to giving installer rights to the app that is doing the installation; right?

A. That's correct.

Q. And in this case the app doing the installation is Chrome; right?

A. In this case, yes.

Q. And on Android any app can be given the right to install other apps; correct?

A. That is correct.

Q. For example, even a calculator app that declared the right permissions could become an installer and install apps on Android; right?

A. That is right.

Q. And if the user slides the toggle we see in Step 4, that

effectively authorizes Chrome to become an installer on that device; correct?

A. That's accurate.

Q. And it's not just the installation of one app. By flipping that toggle, Chrome can install other apps in the future; correct?

A. Correct.

Q. So in your example, we were talking about the -- in your testimony, you were talking about the Wikipedia app. The user may be installing the Wikipedia app here, but in the future the user could be installing other apps; correct?

A. Assuming they didn't abandon the flow, which is an important point.

Q. Assuming the user didn't abandon the flow and the user enabled Chrome as an installer, it's not just the one app the user was installing at the moment that could be installed, the user can also install any number of apps in the future; right?

A. If I understand the setup, yeah. Once that slider is moved over, then there won't be subsequent prompts to anyone to allow Chrome to be an installer.

Q. So, for example, if the user went back to that Nitflix app we were looking at earlier and tried to install it, the user wouldn't see screens 3 and 4 again; right?

A. That's correct.

Q. And you agree with the concept of asking the user to

consent before you allow one app to become an installer on the phone; right?

A. Yes. Users should have to consent before an app can act as an installer.

Q. And that's because the permission to install other apps has pretty significant security implications; right?

A. That's correct.

Q. It's a powerful permission; right?

A. Powerful in the sense that, yes, it has security implications.

Q. And it's a permission that deserves special attention from the user; right?

A. Yeah. Users should have to give consent for those types of powers to be used.

Q. And the reason for this is that an app that has the power to install other apps can later install malware; right?

A. That's possible, yes.

Q. And an app that can install other apps can give attackers powerful capabilities to corrupt the device; right?

A. That's the thing malware can try to do, yes.

Q. And that's a thing malware could actually do; right?

A. It can try to do that. Whether or not it succeeds, depends on a variety of factors.

Q. And your proposals in this case actually do require a user to give consent before an app becomes an installer of other

apps; right?

A. Correct.

Q. Now, your primary concern with these screens 3 and 4 is that they don't apply to preinstalled apps; right?

A. They don't apply to preinstalled apps.

Well, I wouldn't quite phrase it that way. I refer to my original framing in terms of the friction flows need to be proportional. An aspect of that is that Android's current design privileges preinstalled app stores so they don't have to step through any of these friction screens.

Q. Let me ask this a different way.

Your primary concern in Steps 3 and 4, is that they are discriminatory in favor of preinstalled apps; right?

A. That is one aspect of the problem, yes.

Q. And, in fact, at the time you submitted your reports, that was the one and only concern you identified; right?

A. Well, as I mentioned, I think the framing is important.

Q. Professor Mickens, at the time you submitted your report, that was the one and only concern you identified with Steps 3 and 4 here; right?

A. Well, I would say if you look at the report --

Q. All right. Professor Mickens --

MR. OLASA: Your Honor, can we take a look at 208:2 to 208:19?

THE COURT: Of what?

MR. OLASA: Of Tab 1.

THE COURT: Well, you can do it, but I don't find this to be particularly impeaching.

Go ahead.

MR. OLASA: We have a clip of this one, Your Honor, to make it faster. Can we put the clip up?

(Video was played but not reported.)

BY MR. OLASA:

Q. That was your testimony; right? Correct, Professor Mickens?

A. That's correct.

Q. Now, treating preinstalled stores differently when it comes to installation rights is very common; correct?

A. Yes, that's common.

Q. Many operating systems trust the preinstall store; right?

A. Correct, in the sense of, like, they don't put up additional friction screens.

Q. Right. On many operating systems, the preinstall store doesn't see any warning screens; right?

A. Correct.

Q. Like on Apple iOS devices, the Apple App Store doesn't get any warning screens; right?

A. That's right.

Q. And we heard about Fire OS devices by Amazon earlier today. Do you recall that?

A. I do.

Q. And on Fire OS devices, the Amazon Appstore is preinstalled; right?

A. That's correct.

Q. And it doesn't get any warning screens; right?

A. That's right.

Q. It's trusted by the operating system right out of the box; right?

A. In the sense of not generating extra friction screens.

Q. And on Apple's Mac OS, the Apple App Store on Mac is also trusted out of the box; right?

A. Correct, in the same sense of not displaying any additional friction screens.

Q. In fact, your reports don't identify a single popular commercial operating system that does not give the preinstalled app store special installation permissions; right?

A. Well, with the same caveat that what is is not always what should be. That's correct, I don't point that out, yes.

Q. All right. I want to focus on what is.

So based on what is, there isn't a single popular commercial operating system that does not give the preinstalled app store special installation permissions; right?

A. To my knowledge, that's correct.

Q. Now, at the end of the day, Professor Mickens -- can we have Demonstrative 15 up?

At the end of the day, Professor Mickens, over a billion users have successfully navigated these screens; right?

A. I'm not in a position to know the number of users who've navigated these screens.

Q. You know more than half of Android users have navigated these screens; right?

A. I'm not in a position to say either which way.

Q. Well, Professor Qian's report brought this information to your attention; right?

A. That's correct.

Q. And your reply report doesn't claim that his interpretation of the data is wrong; correct?

A. Correct, although it does talk about internal Google sources who say that friction is a significant barrier.

Q. Professor Mickens, I think my question was fairly straightforward.

Does your reply report claim that the data on sideloading is wrong?

A. It doesn't specifically claim that that observation is incorrect.

Q. Understood.

And you, yourself, don't have any actual data on how often users go through these screens; right?

A. I don't have any raw numbers, no.

Q. So we just looked at how Android handles sideloading.

Let's look at what some other operating systems do.

Can we go to Demonstrative 16?

Professor Mickens, you're familiar with the Nintendo Switch; right?

A. Correct.

Q. The Switch is a mobile gaming device?

A. That's right.

Q. And Nintendo has a store on the Switch; right?

A. Correct.

Q. And, in fact, Epic's game Fortnite is available on the Switch; right?

A. I believe that's correct, yes.

Q. And Nintendo does not support sideloading on the Switch; right?

A. Not officially, no.

Q. And you're familiar with the Xbox and PlayStation gaming consoles?

A. I am.

Q. Microsoft makes the Xbox; right?

A. Correct.

Q. And you actually worked at Microsoft; right?

A. I used to.

Q. Yeah. And Sony makes the PlayStation; correct?

A. Correct.

Q. And Epic makes Fortnite available on both these consoles;

right?

A. That's right.

Q. And neither of these consoles allow any sideloading; right?

A. Not officially, no.

Q. And, finally, let's talk about Amazon.

Amazon has the Fire OS operating system we talked about a moment ago?

A. That's correct.

Q. Demonstrative 18, please.

And Fire OS has Amazon's own app store on it; right? We talked about that a moment ago?

A. That's right.

Q. And it doesn't come with Google Play loaded on it; right?

A. You mean the Play Store?

Q. That's right.

A. Correct.

Q. And to make Fire OS, Amazon actually started with the Android open-source code that Google makes freely available to anyone; right?

A. That's correct.

Q. And Amazon made changes to that source code to make Fire OS; right?

A. That's accurate.

Q. And it didn't have to pay Google anything to do that;

right?

A. No. That open-source code is freely available.

Q. And, in fact, Amazon made some security changes to Fire OS that are not in Google's Android; right?

A. Correct.

Q. And if it wanted to, Amazon could have changed those sideloading consent screens we looked at earlier; right?

A. If it wanted to, yes.

Q. Amazon could have implemented either centralized or decentralized notarization; right?

A. That's possible.

Q. But, in fact, Amazon has retained the same sideloading screens we saw when we walked through the Google flow; right?

A. I believe that's correct, yes.

Q. Are these the screens, Professor Mickens?

I'll move on to Demonstrative 19.

Are these the same screens that Fire OS uses?

A. Yes, I believe -- right. So Silk is the browser that you oftentimes see used on those Amazon devices.

Q. And these are -- these are the same consent screens in effect we saw for Google Android; right?

A. Yes. They're very similar, yes.

Q. All right. And, finally, let's talk about Apple's iOS.

And we can go to Demonstrative 20.

Now, Apple doesn't allow consumers to do any sideloading

on the iPhone; right?

A. Correct. That's not officially sanctioned.

Q. In fact, Android has much less restrictions when it comes to sideloading than an iPhone; right?

A. Comparatively, yes.

Q. And you believe that Android and Apple's iOS are roughly equivalent on security; right?

A. I do.

Q. But you agree that popular media outlets sometimes portray iOS as more advanced than other operating systems; right?

A. I'd say that's true.

Q. And this belief is nurtured by Apple's aggressive marketing narrative on security; right?

A. I agree Apple does have a lot of marketing to that effect.

Q. And this marketing by Apple, it influences consumer purchasing decisions; right?

A. It can.

Q. Security is one thing many consumers care about; right?

A. Some consumers, yes.

Q. Are you saying there's some consumers that just don't care about security?

A. No. I'm just saying I'm not sort of like a marketing expert. I haven't done user surveys of how people rank their individual, you know, desired qualities for phones; but, yes,

some people will care about it.

Q. And Apple's marketing narrative attacks Android for allowing sideloading; correct?

A. Among other things. Apple attacks Google for a lot of different reasons.

Q. That's true. Apple attacks Google all the time; right? Apple and Google are fierce competitors; right, Professor Mickens?

A. I mean, in the sense that they both sell phones. I mean, I don't want to weigh into the antitrust issues but, yeah.

Q. Of course. And Apple's marketing narrative on security attacks Android for permitting sideloading; right?

A. That's one of the things that Apple complains about.

Q. If Google dropped the sideloading warnings, Apple would have a field day; right, Professor Mickens?

A. Well, I mean, nothing in my proposal is setting up such a field day as you describe.

Q. You think that Apple might attack Android for dropping these sideloading warnings?

A. Well, I'm not -- I mean, are you suggesting that my proposals would drop those sideloading warnings? I guess I don't understand the context of the question.

Q. If Android were to drop the sideloading warnings, do you think Apple would attack Android in the marketplace?

A. I think that if Google did not replace those warnings with

something that tried to protect users, Apple would make some hay out of that.

Q. Thank you, Professor Mickens.

MR. OLASA: I pass the witness.

THE WITNESS: Thank you.

THE COURT: Okay. Any brief redirect?

REDIRECT EXAMINATION

BY MR. CLARKE:

Q. Professor Mickens, can you hear me okay?

A. Yes, I can.

Q. You were asked some questions at the end there about Apple. Do you recall that?

A. I do.

Q. And you were asked whether Apple and Google compete. Do you recall that?

A. I do.

Q. What do you understand that term to mean in the context of your testimony here?

A. So I'm not an economist and so, you know, I can't talk about what competition means in the antitrust sense.

My understanding as a security expert and an engineer is that both Apple and Google, they, you know, have engineers, they have security people who are working on adding various features to their phone. And so there's sort of like a technical rivalry there, a technical competition. But, you

know, I can't talk about, you know, sort of the antitrust definitions of are they competitors.

Q. Professor Mickens, you were asked a series of questions about centralized notarization. Do you recall that?

A. I do.

Q. And there were five propositions on a slide that Google counsel put in front of you. Do you recall those five propositions?

A. I do.

Q. And you said that you disagree with the way that that was presented on that slide. Do you recall?

A. I do.

Q. Why do you disagree with that?

A. So let's see, let me see if I can remember the five propositions.

So some of the propositions were about cost. So, you know, what would my notarization proposals cost. And I was asked whether I'd evaluated the dollar amount of that, and I answered no. And that's true, I haven't evaluated the dollar amount.

But what I did evaluate in both of my reports is how those proposals would scale. So what does that mean? Like in computer science terms, something scales when you look at how easy is it to make it bigger to handle more users, things like that.

And so I did evaluate how my notarization proposals would scale. And what I observed is that for a company that operates at the size of Google -- right? -- their mission is to organize all of the world's data. When we look at sort of how much my proposals would cause Google to have to scale up their reviewing process, for example, to the extent that happened, I think those scaling costs would be minimal.

And when I looked at, for example, the cost in terms of implementation of changing Android itself to implement my notarization proposals -- well, I've worked on multiple OSs. When I was in grad school, I worked on Linux. When I was at Microsoft, I worked on Windows.

And so I evaluated the sort of the cost of my proposed changes to Android in the context of that experience, and I found that those costs would be quite small relative to, you know, many other changes Google's made to the rest of their infrastructure.

So that was one of the things that was on the slide, and that was one thing that I objected to the characterization of it. In other words, just because I can't give a dollar value, that doesn't prevent me from saying, "Well, for a company that works at Google's scale, this is a reasonable low-lift effort for them to do."

Q. You were also asked -- I believe you were shown Slide 16 of your demonstratives, which had a quote from a Google

whitepaper. Do you recall that?

A. Yes.

Q. And you were asked whether centralized notarization is consistent with aspects of an Android security model. Do you recall that?

A. That's right. And if I recall correctly, that quote, there is the grayed-out text, this is the quote you're referring to --

Q. Correct.

A. -- in the grayed-out text -- oh, thank you very much. Whoever did that, thank you.

So the grayed-out text says (as read):

"A central vetting of developers or registration of users is not required."

And so the question was essentially: Doesn't your centralized notarization proposal violate the ethos, the spirit of that grayed-out sentence. And the answer is no because in the centralized notarization proposal that I made, there is still no requirement that all app developers have to somehow register with Google and must submit their apps to Google.

That requirement's not there in the current way that Android is designed, and that requirement isn't present in either of my notarization proposals, centralized or decentralized.

Q. Professor Mickens, do you believe that your centralized

notarization model would result in opening or closing the Android ecosystem?

A. It certainly doesn't close it. And, in fact, it may end up opening it even more because now more developers might be inspired to submit their apps for review and distribute them through various mechanisms because now the review process has been opened up. And so for developers who were afraid of submitting their app to review because they didn't want to only distribute through the Play Store, my centralized notarization proposal provides more openness.

Q. You were shown a figure from your expert report that had a series of friction screens. Do you recall that?

A. I do.

Q. I think it was Figure 24 from your expert report.

A. Yes.

Q. Do you recall which Android version you used to create Figure 24?

A. I believe that was Android Version 12 that we used in the report.

Q. And do you know whether the friction steps in Android 12 were the same as they were in earlier Android versions?

A. So there's been some slight tweaking there, but they're largely the same.

Q. Do you know whether there were any additional steps that were added or steps that were substracted from Android 12 in

prior versions?

A. I believe there was navigation screen that was removed, like one extra step that a user had to perform.

Q. And you were asked whether individual screens you thought were reasonable. Do you recall that?

A. I do recall that.

Q. In the aggregate, do you view that friction flow is reasonable?

A. Well, I think that's the core point; in the aggregate. So if we look at that workflow overall and we start sort of discounting this and then this and then this, and then all of a sudden it makes it seem like the friction isn't that much.

But, of course, that's not what the user experiences. The user doesn't experience somehow just that, I think, third and four screen in isolation. They experience the whole workflow.

So I think the way of analyzing that friction flow that was presented wasn't actually representative of what users actually experience.

And so, yeah, so when we looked during my direct testimony at my proposed -- my proportionate friction flows, they actually represent something that would really shrink those screens to something that is actually proportional to the amount of risk posed to the user.

Q. You were shown a Switch and Xbox and a PlayStation. Do you recall that slide?

A. I do.

Q. Are any of those devices general purpose computing devices?

A. No. Those are all gaming devices.

Q. Do you consider an Android phone to be a general purpose computing device?

A. I do.

Q. Do you have an understanding for whether the decision not to support sideloading is driven by security as opposed to other business consideration on these platforms?

A. So my understanding is that on gaming platforms, they have certain economic business models such that, for example, sometimes the consoles are sold at a loss; and as a result, the manufacturer of the console wants to make sure they can have certain monetary flows. And so the sort of use models from the user perspective, as well as sort of the economic models underneath it, are much different.

Q. You were asked about guidance from CISA. Do you recall that?

A. Yes.

Q. That's a government agency?

A. That's right.

Q. Do you think that the guidelines issued by government agencies like CISA would be necessary in your alternative scenarios?

A. I think the guidance would look a lot different. I think that the reason why you get guidance like the one that sort of you were presented with is because right now Android is designed in a way that makes it difficult for users to make informed decisions about security.

So that's why if you look at the full context of that paragraph that was there, it's important to look not just to that fist sentence but also the last one too. That paragraph is basically saying: Well, install via first-party stores. That's important. But then also you can get malware through those stores so also look at developer reputation.

I mean, what a mess; right? And in part, that's a mess because Android doesn't provide those clear, concise warnings that speak specifically about whether an app has received a strong security review regardless of its app distribution channel.

MR. CLARKE: Your Honor, subject to any questions from the jury, I have no questions for the witness.

THE COURT: Oh, yes. Ms. Clark?

Is this Number 6?

THE CLERK: I think so.

THE COURT: Okay. I will ask this question and here it is. All right?

Taking into consideration third-party stores and direct installation, are there different kinds of malware that apps

downloaded or sideloaded through these channels may be subject to that apps downloaded through the Play Store would not be?

THE WITNESS: Thank you.

So as I understand the question, whoever asked it, I think what they're asking is: Are there different threats that a user is exposed to in terms of different types of malware depending on the channel, the distribution channel by which that malware would arrive? And the answer is no.

So, in other words, if you look at, you know, different types of malware, ransomware, Rootkits, Trojans, I could list a number of different types of malware, all of those can be distributed via all of the distribution channels that I mentioned.

And, in fact, this is a core reason why, from the perspective of the operating system, and, in fact, from the perspective of the malware scanner, you know, this is why you have to be equally as suspicious about all apps and just think about: What are they going to try to do? You can't just give them a free pass because they come from a particular distribution channel because all of those distribution channels we talked about, they can all be used as vectors to install the same exact kinds of malicious software.

THE COURT: Okay. Thanks very much. Careful on the way down.

This was Question Number 6.

(Witness excused.)

THE COURT: Okay. Who do we have next?

MR. OLASA: Your Honor, Google calls Dr. Zhiyun Qian.

THE COURT: Oh, okay.

MR. OLASA: We're just going to hand out some binders, Your Honor.

THE CLERK: Please stand and raise your right hand.

ZHIYUN QIAN,

called as a witness for the Defendant, having been duly sworn, testified as follows:

THE WITNESS: Yes, I do.

THE CLERK: Please be seated.

THE WITNESS: Thank you.

THE CLERK: Please state your full name for the Court and spell your last name.

THE WITNESS: My full name is Zhiyun Qian. My last name is spelled as Q-I-A-N.

MR. OLASA: May I proceed, Your Honor.

THE COURT: Please.

DIRECT EXAMINATION

BY MR. OLASA:

Q. Professor Qian, what is your occupation?

A. Well, I'm a professor at the University of California at Riverside in the computer science and engineering department.

Q. Do you specialize in any particular area of computer

science?

A. Well, I do research in computer security, and a lot of my research actually focused on Android security specifically.

Q. What subjects do you teach at UC Riverside?

A. Operating systems and computer security.

Q. And do you have any graduate degrees in computer science?

A. Yes. I have a Ph.D. from the University of Michigan.

Q. Have you published research in the field of computer science, Professor Qian?

A. Yes. I've published over 100 articles, and over a dozen of them are specifically focused on Android security.

Q. And putting aside your research work as a professor, do you have any professional experience with Android?

A. Yes. So before I became a professor, I worked for two years in a research lab called NEC Labs where I was responsible for helping develop an anti-malware solution basically for Android.

MR. OLASA: Your Honor, I tender Professor Qian as an expert in computer science, computer security, and Android security.

MR. CLARKE: No objection, Your Honor.

THE COURT: Okay. He's qualified on the topic of security.

Go ahead.

\\\

BY MR. OLASA:

Q. Professor Qian, have you ever received grant funding?

A. Yes, I have.

Q. And did you personally receive this money?

A. No.

Q. What did you do with the grant money that Google has provided to your lab?

A. The grant money is basically provided to the university to sponsor research, and that money is typically paid to my Ph.D. students, you know, in terms of tuition and stipends.

Q. What is the total amount of grant funding you've received?

A. Roughly 270,000.

Q. And taking into account all the time you spent at UC Riverside, what portion are these grants of the total grants you have received?

A. Roughly 5 percent.

Q. Did receiving these grants affect your opinions in this matter in any way?

A. No.

Q. All right. Professor Qian, did you create some slides to help describe your opinions to the jury?

A. Yes.

Q. All right. Let's turn to that first slide.

MR. OLASA: Ms. Clark, can we have control?

\\\

BY MR. OLASA:

Q. Okay. Let's go on to the next slide. I have the controller.

So we'll go into these in more detail, but could you please tell the jury, what are your main conclusions in this case?

A. Sure. So I have three main conclusions as you can see on the screen. First, Android faces significant malware threat.

Second, I've looked at Android's sideloading process. We've been talking about it a lot. And my conclusion is that it's prudent and consistent with industry best practices and security principles that I teach in class.

Lastly, I've evaluated Professor Mickens' proposals carefully, and my conclusions are the alternative security models are less flexible, would introduce new security risks, and impose a burden on Google.

Q. All right. Let's turn to the first conclusion, Professor Qian.

Is malware a problem for all computers or just mobile devices?

A. They're for all computers.

Q. Are mobile devices particularly attractive targets for malware?

A. Yes, they are, just because the sheer volume of mobile devices. In fact, now we have many more mobile devices

compared to personal computers.

And, of course, beyond that, there are several other reasons. For example, nowadays we have many -- much more sensitive information stored on our phone. You know, you have your location, for example, and your phone is always on and always with you. And, you know, malware can use that to, for example, track your physical location, which it wouldn't be able to do in personal computers.

Q. And is malware a greater threat to Android devices as compared to other mobile devices?

A. Yes.

Q. Why is that the case?

A. Well, compared to iOS, for example, there's really only one app distribution channel, which is the official app store.

Now, in Android, we have multiple app distribution channels. We've been seeing that, you know, all this time during the trial. And, you know, malware can get through from any of those app distribution channels.

Q. Why does having multiple avenues of app distribution affect the risk of malware?

A. Well, it simply means there are multiple doors where malware can slip through.

Q. If malware does get on a user's device, what can it do?

A. Well, it can do a lot of different things to harm the users or their devices. You know, they could steal sensitive

information. They could lock up your device, encrypt your files, and demand ransom; or they could, you know, secretly track you.

Q. And are there different types or categories of malware?

A. Yes, there are.

Q. All right. I want to make sure we go through a few of those. Not too many.

So first, what is adware?

A. Well, adware is what you can see on the screen here. It's pretty obvious; right? It's malware basically displaying excessive numbers -- number of advertisements to the point where the screen becomes less usable; right? They're really annoying. I'm sure some of you have seen this before.

Q. And what about ransomware? What is ransomware?

A. Ransomware is where malware would prevent users' access to their devices or their files and unless the user pays some kind of ransom.

Q. So this slide shows something called Cyberpunk 2077 Beta. What is this depicting, Professor Qian?

A. Well, so Cyberpunk was a very popular game launched on PCs, you know, such as Windows, and somehow the users in this case were tricked into thinking that there's an Android version of Cyberpunk. Well, there never was Cyberpunk for Android.

But, unfortunately, users don't know better; and when they actually download and install such apps, what they get is

actually ransomware. In fact, you know, the screen is probably too small to see, but the right screen is showing, you know, the app, you know, displaying certain instructions and force the users to actually pay ransom, otherwise their files will be forever encrypted and it won't be possible -- users won't be able to get the files back.

Q. Okay. And, finally, what is spyware?

A. Well, spyware basically means, you know, you have, like we talked about, a ton of sensitive information nowadays stored on the phone. You know, you have your chat messages. You have your browser, you know, search history. You have, you know, your location. They can even secretly record video and audio using the camera and microphone on the device.

Q. Can spyware steal user banking credentials?

A. Yes, they certainly can.

Q. And what is being depicted on this slide that the jury's seeing?

A. So this is showing sort of another example of deception, which, you know, we've seen over and over and over again; and in this case, it's showing a piece of malware disguised as system update app. And you see that little Google icon there? It's not actually real Google. In reality, this is malware and it's actually secretly collecting information in the background and sending them to the malicious actor.

Q. Now, during Mr. Kleidermacher's testimony, do you recall

him testifying about FluBot?

A. Yes.

Q. And did you review the transcript of his testimony?

A. Yes, I did.

Q. And the jury's heard a lot about FluBot. So just briefly, how does this slide relate to FluBot?

A. Well, again, this is another example of deception, but in this case we see the screen on the left a user is, again, tricked into thinking that there is this, quote/end quote, FedEx app where users are encouraged to download the FedEx app in order to track their packages. Lo and behold, when the user actually clicks on the link, it's actually malware.

But it's really tricky for the users to figure out because as you can see on the right screen, there is that FedEx icon which looks legitimate. But, again, when the user actually installs this particular app, it is FluBot malware actually.

Q. Did FluBot spread through sideloading?

A. Yes, they do, and this is exactly an example of sideloading.

Q. All right. Professor Qian, did you look at the sideloading consent screens in Android?

A. Yes, I did.

Q. And what were your conclusions as to those consent screens?

A. Well, overall, my conclusion is that they're prudent and

consistent with industry best practices and the security principles that are well established.

Q. Okay. So before we get to these sideloading screens and your testimony on that, I'd like to first ask you about preinstalled app stores.

Can Android devices come with a preinstalled app store?

A. Yes, they can.

Q. We heard a lot of testimony about this. What can a preinstalled app store do?

A. They can install additional apps or update apps.

Q. And who configures a device to have a preinstalled app store?

A. Well, it's the OEMs, such as Samsung.

Q. And can an Android system come with more than one preinstalled app store?

A. They certainly can, and it does happen in practice.

Q. I think Professor Mickens covered this, but if a user tries to download an app from a preinstalled app store, will the user get any warnings from the operating system?

A. No.

Q. Why won't the operating system issue a warning in that situation?

A. That's a good question. So in this case, the user is actually purchasing a device from the OEM, let's say from Samsung, and the user is already trusting the OEM, you know,

Samsung, that's placing whatever preinstalled app store is on the phone. So there is already that trust relationship that's already established -- right? -- if you think about it.

And, in fact, if you purchase a Samsung device, you would expect that you'll be able to install applications right out of the box, otherwise it would be very awkward.

Q. Now, do other operating systems also have the concept of preinstalled app stores?

A. Yes, they do.

Q. And for these other operating systems, will the user see any warnings if they attempt to install apps from a preinstalled app store?

A. No, none of the other operating systems show a warning for their preinstalled app stores.

Q. So is the Android approach to preinstalled app stores consistent with what other platforms do?

A. Yes, it is.

Q. Now, on Android, if the user wants to install apps from outside a preinstalled app store, we've seen that users can sideload, so I don't want to rehash that ground, but I want to briefly go to the sets of screens and get your testimony on them, Professor Qian.

So, first, I want to ask you about -- I want to ask you about this screen, this installation consent screen. And the jury has seen some videos and demonstratives before.

Can you remind the jury, what does this screen show?

A. Well, this is -- like you said, it's an installation consent screen. This is displayed after the user has granted the sideloading permission to a particular app. This is basically the screen that a user would see after the sideloading permission is granted.

Q. So I want to make sure we're clear on this.

So if a user downloads a sideloaded app store and consents to that sideloaded app store installing other apps, for future installations, is this the only screen that the operating system shows for an installation?

A. Yes, this would be the only screen.

Q. And in your opinion, is this consent screen a reasonable security precaution?

A. Yes, it is. And I think Mickens and I agree on this point.

Q. Now, why is the screen needed if the user has already granted consent to a particular installation source?

A. Well, it's because without the screen, the app, you know, let's say, you know, in this case a third-party app store or any other sideloaded apps, could then install any number of apps subsequently without user knowledge. And, you know, even a calculator app with this permission can then basically silently install malware.

Q. So let's talk about the way a user can set up a store to

become an installer.

What do these screens show, Professor Qian?

A. This is showing basically how the sideloading permission would be granted to a specific app, let's say a third-party app store.

And the first screen here shows basically -- we've seen this before -- it's basically directing the user to the settings in order to authorize the sideloading permission.

Q. And as a security researcher, do you think it is appropriate to ask user consent before allowing an app to become an installer on a device?

A. Yes, I think it's completely reasonable. And, again, I think Professor Mickens and I agree on this point.

Q. So what could happen to users, from a security perspective, without this consent flow?

A. Well, this would mean that a user would not have a moment to reflect about the decision that they're about to make, which is sideloading.

And we all know sideloading is a dangerous operation, and it is widely accepted in the industry and academia. In fact, this sideloading permission is not about sideloading a particular app. It's about enabling a particular source, in this case Google Chrome, to install any number of apps subsequently.

You know, you could install, let's say, Wikipedia today

and tomorrow you could be installing malware. You could be installing malware from the same exact app source.

Q. You see on the right that there's a toggle that says "Allow from this source." And you used the word "source" a moment ago. From the Android's operating system perspective, what is a source?

A. Well, a source is basically an app that can act as an installer. Right? It's able to install other apps. So in this case, if you're, let's say, installing Wikipedia from Chrome, well, it's the Chrome that's the source as opposed to Wikipedia.

Q. Now, you mentioned a moment ago that installing -- the ability to install apps is a dangerous permission.

Does Android ask users for consent for other dangerous permissions?

A. Yes.

Q. Can you give the jury some examples?

A. Well, I think if you've used Android devices before, you'll see things like, you know, when an app is trying to access your GPS location, you would see a warning screen. Right? Or if the app is trying to access your -- it's a camera -- right? -- you'd be warned as well.

Q. And is the ability to install an app more dangerous than these other permissions you've described?

A. Yes. In my view, being able to install additional apps

would be considered more a dangerous operation than, let's say, accessing your GPS location.

And, in fact, this is consistent with what Professor Mickens has said. You know, friction should be consistent with the level of risks. In this case, we're looking at a very dangerous operation of sideloading, which is, again, not about installing one particular app; it's about this app source, in this case Chrome, being able to install any number of apps subsequently. Right?

And given that, it is perfectly reasonable to have more friction compared to a regular permission in Android.

THE COURT: Okay. Let's take our afternoon break. We'll come back a little bit after 2:15.

THE CLERK: All rise.

(Recess taken at 2:00 p.m.)

(Proceedings resumed at 2:16 p.m.)

(Proceedings were heard out of the presence of the jury:)

THE COURT: Bring the jury out.

(Proceedings were heard in the presence of the jury:)

BY MR. OLASA:

Q. Professor Qian, are all apps on the Google Play Store reviewed for malware?

A. Yes, before they're published on Google Play.

Q. Can you briefly explain to the jury what that review process consists of?

A. Well, at a very high level, there's this automated review process, you know, using state of the art, you know, program analysis and machine-learning algorithms. I won't get into the details. And there's this complimentary human review process that goes along.

Q. And are all new apps on the Google Play Store reviewed by a human?

A. Yes.

Q. Does the Google Play Store still have malware?

A. Yes.

Q. But is Google Play Store a relatively safe place for apps?

A. Yes, because they have, you know, according to various sources, lower malware rate compared to other app stores or sideloading channels.

Q. Are all sideloaded apps reviewed for malware?

A. No.

Q. And how does that difference affect the risk of sideloading as compared to downloading from the Google Play Store?

A. Well, that means by design, sideloaded apps would have a higher chance of being malware because if they're not reviewed by any entity, then it's very likely -- you know, it's likely that some of them would be malware and nobody would have caught them.

Q. Does academic research conclude that sideloading is risky?

A. Yes.

Q. And is there a consensus on this point?

A. Yes.

Q. And did you also consider the views of industry participants on the risks of sideloading?

A. Yes, I did.

Q. And why did you consider these views?

A. Well, because they are the stakeholders, like OEMs and antivirus companies, that have an interest in the Android users.

Q. All right. So, Professor Qian, what does this slide show?

A. This is showing a number of quotes from various segments in the industry. For example, Verizon is a wireless carrier in the U.S. that sells Android. Lookout is an antivirus company that specializes in mobile security. Samsung we all know is an OEM that manufactures Android devices.

And in this case, for example, Samsung is telling their users sideloaded apps from outside sources can be a little like the Wild West, unregulated and potentially hazardous.

Q. Now, did you analyze any information from the plaintiff, Epic Games, on whether sideloading is risky?

A. Yes, I did.

Q. What did you find?

A. Well, in this case after the Fortnite installer app has been sideloaded successfully through the browser app, we see

that it generates a warning to the users saying that, "Oh, your browser has been granted the sideloading permission and please now disable it" because, you know, you want your device to be secure. You don't want to enable sideloading all the time.

Q. And how did this message relate to your opinions in this case?

A. Well, it means that there is a general consensus, you know, even from Epic, that sideloading is risky.

Q. So turning back to the sideloading warnings.

In your opinion as a security researcher, are they unduly difficult?

A. No, I don't think so.

Q. And have you compared the sideloading screens to how sideloading is handled on other mobile platforms?

A. Yes.

Q. I think the jury has already heard that iOS doesn't allow sideloading. So are Android's consent screens less restrictive than what iOS does?

A. Yes, because by definition iOS doesn't allow sideloading.

Q. And earlier with Professor Mickens we talked about Amazon's Fire OS. Do you recall that?

A. Yes.

Q. What is Fire OS?

A. Well, Fire OS is an operating system now under Amazon, and

that operating system code is taken from the Android open-source and they made, you know, changes to it and now brand it as Amazon -- sorry -- as Fire OS.

Q. And is Amazon free to make any changes it wants to the code?

A. Yes, they can. In fact, they do, as we just talked about.

Q. And how does Fire OS's approach to sideloading compare to Google's?

A. It is basically the same two identical screens that we have seen.

Q. And, Professor Qian, have you also looked at any data regarding the proportion of devices that have enabled sideloading?

A. Yes, I did.

Q. And where did you obtain that data?

A. It's from Google's Joint Guard data.

Q. And what do the data show?

A. Well, it showed, I believe -- yes, next slide -- that globally, this is data actually for November 2021, it's showing that worldwide the percentage of devices was at least one app that has enabled sideloading.

So that means over a billion users -- right? -- because This is, again, worldwide data, excluding China, by the way -- more than a billion users who have successfully navigated the unknown source flow that we've been talking about all this

time.

Q. And is it significant to you that more than half of users had enabled sideloading at least once?

A. Yes.

Q. Why?

A. Well, if more than a billion users can navigate through that flow, then it must not be too difficult.

Q. All right. Let's turn to certain security principles.

Did you assess Android's consent screens against any computer security principles?

A. Yes, I did.

Q. Which principles?

A. Well, there are three main principles I show here: Defense in Depth, secure defaults, securing the weakest link. And I'm going to explain them in more detail in just a bit.

Q. Let's start with Defense in Depth. What is Defense in Depth?

A. Well, Defense in Depth is this idea where you want to introduce multiple layers of defense in case one of the layers is bypassed by the attacker so that you still have these other layers that have a chance to stop the attack. It's a very simple and well-established security principle in my field.

And just like what you see here on the screen, a good analogy to understand this is, you know, if you want to defend your castle, you want to have your wall up, you want to have

your moat, and you also want to have your guards -- right? -- so in case one of those layers of defense fails, you still have other layers.

Q. Are the sideloading consent screens we're looking at consistent with this principle of Defense in Depth?

A. Yes, it is. I can explain. You know, I think we all agree. Professor Mickens and I also agree on this point.

You know, operating system is an important layer of defense, but it doesn't mean that we should let go these other layers of defense, which in this case, you know, we know sideloading is a very dangerous operation and it warrants a sideloading -- sorry -- a warning.

Q. What about the principle of secure defaults? What is that principle?

A. Well, the principle is stating, yes, if you have all of your layers of defense, which is all great, but if you don't enable them by default, then it wouldn't work.

And, conversely, if you have dangerous operations that can undermine these layers of defenses, they don't want to enable those dangerous operations by default. Right?

So similar to the same analogy here. Even if you have all these good layers to defend your castle, but if your drawbridge is down, is open, then attackers can just walk right in -- right? -- and bypassing all of your defenses. That's why we want the drawbridge to be up or closed by default.

Q. Do Google's sideloading consent screens comply with this principle of secure defaults?

A. Yes.

Q. And can you explain why?

A. Well, basically, like I mentioned earlier, sideloading, you know, or granting an app to be able to install other apps in general is a dangerous operation. I think we all agree. And since that is a dangerous operation, just like any other permissions that Android has, we don't want to grant that permission by default. We want to grant that permission only when it's necessary.

Q. All right. Professor Qian, what is securing the weakest link, and why is there a barrel on the screen?

A. Well, I can explain.

What the idea of weakest link in the computing system is that attackers will always gravitate towards the weakest part of your system. Just like water would gravitate towards the lowest hole in the barrel; right?

So if you don't secure the weakest part of your system, then it doesn't matter how secure the rest of the system is. That's why we have this principle called securing the weakest link.

Q. And on consumer devices, what is typically the weakest link?

A. Well, oftentimes it is the user, a human being considered

the weakest link. Why? Well, because humans are often deceived or tricked into doing things that allow malware or attackers an advantage, you know, such as installing malware.

Q. Do the sideloading consent screens comply with the principle of securing the weakest link?

A. Yes, because it's exactly trying to help give the user an opportunity to think and reflect on this dangerous operation of sideloading or installing additional apps. That's a very dangerous operation.

Q. Now, Professor Mickens testified about another Google security feature called Google Play Protect. Do you remember that?

A. Yes, I did.

Q. And Mr. Kleidermacher also testified about that. Do you recall that?

A. Yes.

Q. What is Google Play Protect?

A. Well, at a high level, it is Google's antivirus or malware scanner.

Q. And does Google Play Protect try and protect users who download apps from outside the Play Store?

A. They do try to do that.

Q. And how does Google Play Protect work for apps that are downloaded from outside the Play Store?

A. Well, they're going to be checked against what's called a

block list -- right? -- which is curated at the back end of Google, which basically contains a list of known malicious apps. And if the app that's trying to be installed on the device is on the block list, then the app installation would be denied.

Q. Now, do you recall Mr. Kleidermacher testifying about the effectiveness of Google Play Protect versus the Google Play Store?

A. Yes.

Q. What is your opinion on the effectiveness of Google Play Protect as compared to the Google Play Store?

A. Well, Google Play Protect is -- for off-Play apps is inherently less effective compared to Google Play's protection.

Q. Can you tell the jury why?

A. Well, the simple reason is on Google Play, every single app would have to be vetted or reviewed through a rigorous process before publication. So if an app is already on Google Play, you know, it has gone through this full-blown app review process; whereas for Play Protect for off-Play apps, it's entirely possible that the app has never been seen by Google before.

In fact, malware can use advanced techniques, such as polymorphism, to try and generate a large variance of malware that look different, every single one of them would look different, and yet they're performing the same malicious

operation. It would be very difficult to catch all such malware instances ahead of time and review them.

Q. Are there differences in how aggressive the Google Play Store review process is as compared to Google Play Protect's review process?

A. Yes. There is some fundamental difference there.

Q. And can you explain that difference to the jury?

A. So for the off-Play apps, the system, the AI system, or the machine-learning model would have to be necessarily tuned to be less aggressive in flagging malware.

Why is that the case? Well, because Google doesn't have a relationship with off-Play apps -- right? -- unlike apps that are submitted to Google Play.

And if Google somehow, some way made a mistake about flagging a benign app as malicious, what does that mean? It means that it's giving that app a death sentence. That app is no longer distributable anywhere else, not just from Google Play. It won't be distributed -- Google would basically block that app from being installed from any arbitrary distribution channel.

Q. Does the Google Play Store also have information about the app developer as part of its review process?

A. Yes.

Q. Does Google Play Protect have similar levels of information?

A. No. Like I just mentioned, you know, off-Play apps can be any apps, can be malware -- can come from malware authors or come from anonymous developers, and they could be generated even automatically using sophisticated techniques. And malware can also generate a large number variants of them in just a matter of minutes.

Q. In your opinion, is Google Play Protect sufficient to ensure user security for apps outside the Play Store?

A. No.

Q. And does the existence of Google Play Protect mean that the sideloading consent screens are unnecessary in your opinion?

A. No. It goes back to the security principle that we just talked about: Defense in Depth. Right? You don't want to take away one important layer of defense, especially considering that the other layer of defense is imperfect.

Q. All right. Professor Qian, have you evaluated Professor Mickens' proposals in his expert reports?

A. Yes, I did.

Q. What was your overall conclusion based on the information that Professor Mickens provided?

A. Well, I think the proposal sounds simple, but what's really happening behind the scene is actually a lot more profound than what it looks like. And after some careful analysis, I've arrived at the conclusion that the proposals are

less flexible, would introduce new security risks, and impose burden on Google.

Q. So let's start with centralized notarization. What is centralized notarization?

A. Well, as we can see here, now under this model, Google would become the one and only reviewing entity for the entire Android ecosystem for the universe of Android apps. And basically everybody -- every developer would have to submit their app to Google for review and receive sort of the token that Professor Mickens was talking about. And the key here represents sort of the approval, the seal that Google is able to sort of give to a particular app.

Q. How is the centralized notarization proposal different from what happens today on Android?

A. Well, today every app store can review the apps from within its own app store. Right? They wouldn't have to go through Google to get them approved.

So, for example, if you have Galaxy Store, today all of the apps are reviewed by Samsung within the Galaxy Store; and since they're also preinstalled on Samsung devices, there would not be any warning.

But under the new model, if a user would download apps from the Galaxy App Store and those apps are not reviewed by Google, well, then there's going to be a warning.

Q. Is this the warning that Professor Mickens proposed in his

reports?

A. Yes.

Q. And would any app not reviewed by Google receive this warning under Professor Mickens' centralized notarization proposal?

A. Yes. Regardless of whether the app is distributed through the Play Store or Galaxy App Store, or anywhere else, as long as that app has not been reviewed and approved by Google, this warning would be displayed.

Q. Now, would implementing centralized notarization be a significant change in the design of the Android operating system?

A. Yes, it would be a significant change. Like I mentioned, this may look like a simple change but it's not. There's actually profound ramifications on the entire Android ecosystem on all the stakeholders. Right? It doesn't just affect Google. It affects also the OEMs, the users, and developers.

Q. So how would this centralized notarization proposal affect OEMs?

A. Well, I think we talked a little bit about this before. So today OEMs have the freedom to choose which preinstall app stores to include on their devices and which of those preinstalled app stores to trust.

In the new model, OEMs would effectively lose that ability. Right? Even if they preinstall app stores on their

devices, if those apps have not been reviewed by Google, then they're still going to trigger a warning.

Q. And based on how Android is designed, as a technical matter, as a technological matter, would Google need OEMs to consent to this proposed change?

A. Yes, they would have to agree because, you know, that's basically causing OEMs to lose some abilities. So I would imagine OEMs would want to negotiate and would want to discuss the change.

Q. What about app developers? How does this proposal of centralized notarization affect app developers?

A. Well, it's somewhat similar in the sense that developers, you know, previously they can submit their apps to different app stores, you know, to Google Play, to Galaxy App Store, anywhere else -- right? -- for review. And, for example, on Galaxy App Store, if the app has been accepted and approved on Galaxy App Store, well, then there would not be any warning.

But under the new model, they would all have to submit their apps to Google to get it reviewed and approved in order to enjoy the low-friction installation experience.

Q. Now, how would this model affect users?

A. Well, it's more or less the same idea. Users today can choose to download from the trusted app store, such as Galaxy App Store, and enjoy low-friction experience. And now this change is taking away users' ability to trust certain

preinstalled app stores.

Q. How would this change affect a user's ability to use a sideloaded app store?

A. Well, it's kind of similar. So previously -- today users are able to sideload any app stores; and as long as they enable sideloading for such an app store, there's going to be no warnings for subsequent installations.

However, in the new model, they will see a warning for every single app that has not been approved by Google. So imagine if it's from the Galaxy App Store again, you know, if you wanted to download 50 apps from the Galaxy App Store, if those 50 apps have not been reviewed by Google and approved, well, a user is going to see 50 different warnings every single time for the app that they wanted to install.

Q. And, Professor Qian, are there security risks associated with this proposal of centralized notarization?

A. Yes, there are. And, interestingly, I think Professor Mickens just testified a moment ago that it's going to either maintain security -- that the proposed changes is either going to maintain security or improve security. I disagree with that assessment.

Q. Why do you disagree?

A. Well, there are a couple reasons. I can give two reasons here.

First, it's possible that after an app has been approved,

it's going to turn malicious at a later point in time. Okay? And this does happen in practice, by the way. And it doesn't even -- the app doesn't even have to change its signature. It would still look like it's the same exact app that has been distributed before.

Q. How could an app that's already been distributed change its behavior and become malicious?

A. Well, malware -- there are sophisticated malware tactics that can be employed. One of them, for example, is called Hotfixes.

Q. And through Hotfixing could an app that was originally benign update itself to become malicious?

A. Yes, exactly.

Q. How does this possibility relate to Professor Mickens' centralized notarization proposal?

A. Well, basically that means, you know, if Google has previously approved an app, generated a token for that app, it doesn't mean that app is going to be safe forever. It just -- it won't be able to make that kind of certification.

Q. To address this risk, would Google have to monitor all apps outside of the Play Store?

A. Right. So in order to mitigate that risk, Google would have to continuously monitor all of the apps that it has previously reviewed and approved, including apps that are within the Google Play Store and outside of the Google Play

Store.

Q. Does centralized notarization raise any other security risks?

A. Yes. There is one other risk. You know, I think we talked about users sometimes can actually see more warnings under the new model. Right?

For example, I mentioned today when you install apps from the Galaxy Store, you would not see any warning; but in the new model, you might see a lot of different warnings, one warning for every single app that is not been reviewed by Google.

Okay. So under that model, it's possible that a user would become desensitized to those warnings. And what's going to happen? Well, the users are going to be trained or self-trained to skip those warnings. They're just going to click "Yes" and "Yes" and "Yes," "Install."

And when that happens, it's going to be very bad for the overall security. Right? Because when real malware shows up, it would be that same warning screen and the user would still click "Install," "Install," and it would be infected.

Q. Professor Qian, are you aware of any modern operating system that permits sideloading in which one entity assumes responsibility for reviewing all apps on the platform?

A. No, I've never seen one.

Q. And do you think Professor Mickens' centralized notarization proposal is a sound proposal?

A. Well, again, it may sound like a simple and, you know, intuitive proposal, but it's actually a very complicated proposal as I just laid out.

I think there are some real issues; right? Because it's not a simple change. It affects the entire Android ecosystem. And whenever we make such a systemwide change, you need to do a very careful analysis about the ramifications.

Q. Did Professor Mickens do that analysis?

A. I don't think so.

Q. All right. Let's turn to decentralized notarization.

How does Professor Mickens' decentralized notarization proposal differ from centralized notarization?

A. Well, in the decentralized notarization, we see that Google is no longer the reviewing entity approving apps. Instead, now there are these sort of trusted reviewing entities, third-party reviewing entities, that Google would supervise, and it's those third-party reviewing entities that actually go and review those apps.

Q. Does decentralized notarization suffer from all the same issues we were talking about with respect to OEMs and users and developers?

A. Yes, it's the same idea.

Q. Are you aware of any modern operating system that has implemented decentralized notarization for app review?

A. No, I have not.

Q. Does that concern you?

A. It does concern me in the sense that, you know, again, this is a systemwide change and it doesn't just affect Google. It affects all the stakeholders in the Android ecosystem.

Whenever such a big change is about to be made, we would like to get some more assurance about, you know, what's going to happen, the ramifications, the impact, or any potential negative security consequences.

Q. Would decentralized notarization lead to overall lower security than today?

A. Yes. There can be a number of issues there.

Q. How could that happen?

A. Well, I can talk about two issues here. One, it's what's called race to the bottom, which I'll explain what it means, you know, among different reviewing entities; and, two, there is an increased risk of stolen keys when you have multiple reviewing entities. And, again, I'm going to break down what I mean by that.

Q. Let's first start with the race to the bottom. What's the concept there?

A. Well, let's imagine if there are 10 reviewing entities. Okay? If one of the reviewing entities decides to approve an app; whereas, all the other nine entities decide to reject that app, what happens? Well, the app is still going to get that notarization token where the app can use -- where the app

developer can use to distribute that app and potentially harm users.

Q. How could that affect user security?

A. Well, in this case the reason the other reviewing entities have decided to reject that app is probably because there's something wrong about the app; but now that we have multiple approving -- reviewing entities, as long as one of them approves the app, then the app would be able to get a pass.

Q. All right. Let's turn to this other point of key theft. Can you explain that to the jury and what they're seeing on this slide?

A. Okay. So we briefly talked about the keys here. All right. The keys are basically where -- the keys are basically used by the reviewing entities as sort of the mechanism to sign or to attach a token to an app to prove that the app has gone through the app review. Right?

But if that key is stolen, in this case the red key on the screen is stolen, then what's going to happen is the malicious actor can use that stolen key to sign a bunch of other malware and distribute them.

Q. And would that malware get a low-friction install experience under Professor Mickens' proposal?

A. Yes. In that case, it would create a false sense of security because users are thinking that, "Oh, these are apps that have been reviewed and, therefore, there's no warning and

they must be safe." Whereas, in practice, these are actually signed or sort of reviewed by the malicious actor and they're just malware.

Q. And would Google know that this key theft had occurred?

A. Presumably at some point when somebody notices this, they're going to go back and realize, "Oh, some key is actually stolen." But by then, it probably is too late because maybe, you know, lets say millions of apps could have been signed by that stolen key and the harm could have already been done.

Q. Is the risk of key theft just something hypothetical or is it an actual risk in the real world?

A. Interestingly, the key theft issue is actually very common. I know Professor Mickens has talked about the web certificate domain where it's a decentralized system and, you know, there are multiple signing authorities and so on. It's in some ways similar to the decentralized notarization and there, key theft is such a common issue. It happens all the time; and when that happens, you always have security issues.

And, in fact, in the app review world, when signing keys are stolen, it could even be worse because we're talking about whether an app has been reviewed or not, whether they're malware or not. Whereas in the web certificate case, we're just talking about whether -- we're just talking about the identity of the website, which is very different.

Q. Thank you, Professor Qian.

MR. OLASA: Your Honor, I pass the witness.

THE COURT: Okay. Cross.

CROSS-EXAMINATION

BY MR. CLARKE:

Q. Good afternoon, Professor Qian. Can you hear me okay?

A. Yes.

Q. Great. Thanks.

So, Professor Qian, you're being compensated by Google for your participation in this case; is that right?

A. Yes.

Q. You're being compensated by $600 an hour? Is that your hourly rate?

A. Yes.

Q. And you've worked for approximately 200 hours on this case so far?

A. Probably.

Q. So you've been compensated in the amount of roughly $120,000 so far in this case?

A. I haven't tracked, but could be.

Q. At least as of the time of your deposition; is that fair?

A. Sounds reasonable.

Q. Okay. I want to ask you some questions about the data that you cited, the 53 percent. Do you recall that?

A. Yes.

Q. So I've gone ahead -- you should have a binder in front of

you. If you look at Exhibit 7196 in that binder. I think it's just the same version of that 53 percent chart that you showed us in your demonstratives. Let me know if you have it there.

You might have two binders. One's going to be your deposition and your report. The other is going to be a couple documents.

A. Can you say the exhibit number again?

Q. Yeah. It's 7196.

A. (Witness examines document.) Yes.

Q. Okay. You got it?

A. Yep.

Q. And is that the chart that you showed in your demonstrative a little bit earlier?

A. Yes.

Q. And you testified this chart indicates that there are over a billion users worldwide who have enabled the unknown sources warning in some way; is that right?

A. Correct.

Q. Okay. When you created this chart, did you look into how many countries there are where there's low Internet connectivity prohibiting people from being able to actually download through official stores like the Play Store?

A. No, I did not look at that specifically.

Q. Did you look into how many countries there are worldwide where the Google Play Store has been banned?

A. Well, I know that the data would exclude China because China has banned Google services.

Q. Are you aware of any other countries where Google Play Store has periodically been banned by the government?

A. If I understand correctly, Iran is another example.

Q. Okay. And how does that factor into your data here, your 53 percent? Do you know?

A. Well, my understanding is that, you know, for example, Chinese Android devices would not even show up in the data. So it would not affect my conclusion.

Q. So there are approximately 100 million people who live in Iran; is that correct?

A. I'm not aware of the exact number. Sorry.

Q. Some significant percentage of those people own Android devices; is that fair?

A. Probably.

Q. And those individuals are not able to download apps through the Google --

THE COURT: Well, he doesn't know any of this. Okay? So let's skip Iran. This is not his area of expertise.

BY MR. CLARKE:

Q. So you didn't look into --

THE COURT: We're going to finish this witness today, so plan accordingly. And by "today," meaning 3:30. Okay?

MR. CLARKE: Okay. Understood.

THE COURT: All right. Go ahead.

BY MR. CLARKE:

Q. So did you look into how many people -- when you were preparing this data that you presented, did you look into how many people worldwide are forced to share apps via peer-to-peer networks rather than downloading from some sort of a wireless or Internet connection?

A. No, I didn't look at that data specifically.

Q. Are you aware that there are large countries where people don't have access to Internet connectivity and are forced to share apps via peer-to-peer networks?

A. Possibly.

Q. Are you aware that India is one such country that has a large population?

A. I've heard of India using peer-to-peer app installations, yes.

Q. So people in India who are using peer-to-peer app installation would be included in this 53 percent; is that fair?

A. I presume, yes. If --

Q. Do you know whether -- sorry. Go ahead.

A. I'm sorry.

If their phones are actually eventually connected to the Internet, because that's how Google is able to collect data, otherwise it would not be counted in the data.

Q. Okay. But people in India who don't have access to Internet connectivity and are forced to share apps via peer-to-peer installation, they would be included in the 50 percent figure that you're including here; is that fair?

A. If those devices eventually connect to the Internet, otherwise they would not be included in this data.

Q. Understood. And the same would be for another country like Indonesia?

A. Yes.

Q. Okay. So this data is based on a spreadsheet that Google provided you; is that correct?

A. Yes.

Q. And you called that Droid Guards data; is that right?

A. Correct.

Q. Okay. I'd like to look at that spreadsheet if we could. Unfortunately, it's too large to print off and put in front of you, so we're going to try and put it up on the screen. Hopefully you're able to see it.

A. Sure.

Q. So this is Exhibit 8607. Do you see that in front of you?

A. Yep.

Q. And there are a couple of columns here in Exhibit 8607. So there's a Column A, which seems to be "Country Codes"?

A. Yeah, I understand.

Q. Okay. And there's a Column B, which is "Model." Do you

see that?

A. Yep.

Q. And then there's a Column C, which is "Number of Devices with more than zero from unknown sources." Do you see that?

A. Sure.

Q. And then there's "Number of devices." That's the total number of devices for that model; is that right?

A. Yes.

Q. And then there's a percentage that has been calculated. Do you see that?

A. Yep.

Q. All right. I'd like to filter here -- I'd like to start if we can filter by the country. So we're going to filter this data.

And if we scroll down in the filter fields here to the Us, there's a country that's called unknown. Do you see that?

A. Yes.

Q. Do you have any idea for what's in that unknown column?

A. I'm not sure.

Q. So if it would be possible to filter out everything but the unknown, I'd like to see how many devices are showing up as unknown.

So if we go ahead and highlight Column D here. And then in the lower right-hand corner, there should be a sum. I don't know if you can see that.

A. Yes, I do see that.

Q. So there are about 880 million devices that are in the unknown column; is that right?

A. It appears to be.

Q. Do you have any idea where they are?

A. I'm not sure.

Q. Okay. That could be countries where people are predominantly using peer-to-peer downloads; is that right?

A. I don't know one way or the other.

Q. Okay. If we could unfilter and go back up to the top.

So the first country here is AD. Do you happen to know what "AD" stands for?

A. I can't remember.

Q. I think that AD might be the Principality of Andorra. It's a small European country.

So I just want to kind of go through and see what we see in these models as we go through the rows one by one.

So the first thing I notice is you see that row 7 seems to be a Smart TV?

A. Yes, I do.

Q. Do you have an understanding that your data includes Smart TVs?

A. Yes.

Q. So if we go a little bit further down into the Bs, you'll see a series of rows here that say Bravia 4K. Do you recognize

Bravia as a Smart TV brand that's made by Sony?

A. Yes.

Q. So there are going to be Andorra and Smart TVs in this data set as well?

A. Yes.

Q. Okay. Do you have any understanding whether car entertainment systems are included in this data set?

A. I'm not sure.

Q. Do you think we could find some car entertainment systems if we looked?

A. Possibly. I don't know.

Q. I want to go a little bit further down into the Cs. If you stop right there, row 82 there seems to be a Chromecast. Do you see that?

A. Yes, I do.

Q. A Chromecast is not a mobile device, is it?

A. I think it's used for projecting screens onto a Smart TV.

Q. Okay. So it's not a mobile device; is that the answer?

A. I guess so.

Q. Do you have any understanding for how many Chromecasts are included in your 53 percent data?

A. I haven't checked.

Q. Do you have any understanding for how many Smart TVs are included in your 53 percent data?

A. I haven't checked carefully.

Q. Do you know whether there are any other types of appliances that are included in your data?
A. Even if there are, it wouldn't change my conclusion.
Q. Your conclusion that over a billion users of devices worldwide have enabled unknown sources?
A. Even if it's not 1 billion, let's say it's 500 million, it would still support my conclusion.
Q. And what's the basis for that?
A. Well, 500 million compared to 1 billion is not a huge difference to me.
Q. So, Professor Qian, I'd like to back up a little bit.

You had some testimony about friction. Do you recall that?
A. Yes.
Q. Now, when you were looking at the unknown sources flow, there was one particular piece of data that you wanted for purposes of your report, but you couldn't get access to it because Google didn't produce it. Do you recall that?
A. Right. My understanding is Google simply doesn't have the data.
Q. Right. And as a security researcher, you have to go by the data; right?
A. Well, we can work with the data that are available to us. The data is nice to have as an additional piece of evidence, but the existing data and the evidence that I have already

support my conclusions.

Q. When you were deposed, do you recall testifying under oath "As a security researcher, I have to go by the data"?

A. Yes.

Q. You were interested, in particular, in the exact number of potentially harmful applications or malware that was avoided because of the unknown source warning; right?

A. Yes.

Q. Okay. In other words, if a user decides to abandon the unknown source warning, how many instances of that are really successful in the sense that some malware or PHAs have been avoided; right?

A. Correct.

Q. And you were informed that Google doesn't have that data; right?

A. Correct.

Q. And that data would have helped you analyze whether the friction from the unknown sources flow is actually proportionate to the risk associated with the malware being downloaded; right?

A. I' sorry. Can you say it again?

Q. That data would have helped you analyze whether the frictions associated with the unknown sources flow is actually proportionate to the risk of the malware being presented; right?

A. Well, even without the data, I would already say that the current unknown sources flow is already consistent with that.

Q. I'm sorry. Your understanding is that the security warnings and prompts that are displayed for unknown sources during the installation process are designed to protect users from security risks; right?

A. Yes.

Q. And you asked for data that would have allowed you to compare the friction with the level of risk; right?

A. Yes.

Q. And you were told Google doesn't have that sort of data?

A. That's true, but we have other kinds of data.

Q. Okay. But Google doesn't have data showing how many PHAs are actually being avoided by this unknown sources flow; correct?

A. Not that specific data, that's right.

Q. Your report actually has some data that's relevant to this. Do you recall that?

A. Yes.

Q. Do you recall that your report states that 62 percent of users shown an unknown source warning enable unknown source installations and continue with the installation process?

A. Correct.

Q. And that means that 38 percent of users who are shown an unknown source warning abandon that process; right?

A. Sure. There could be many reasons that they abandon.
Q. So out of every 100 users that go to download something outside of the Play Store who are presented with an unknown source warning, according to the data in your report, 38 of them would abandon that process?
A. Yes. Again, for various reasons.
Q. And you don't have any data on how many potentially harmful applications they are avoiding when they abandon that process; is that right?
A. Well, the data was not available to us.
Q. You don't have any data on how many completely benign applications are being avoided when they are being canceled when they abandon that process; is that right?
A. That's right.
Q. And you testified a few minutes ago on your direct that users sometimes get fatigue with all of these warnings; right?
A. That's right.
Q. They'll just start clicking through?
A. Yes.
Q. And do you think more warnings is going to make people more fatigued?
A. Well, not necessarily more warnings, but repetitive warnings.
Q. Repetitive warnings. So a series of warnings that are all intended to achieve consent for the same thing; right?

A. No. I would say the same exact screens shown over and over again would be considered repetitive.

Q. And when users are forced to navigate through screens over and over and over again, over time, they'll simply start clicking "Okay"; right?

A. Not -- not -- I think the definition is different. My definition is it's the same exact screen shown over and over again.

I think in the current Android security model, you only see the unknown source warning once per source; whereas, in the new model, you're going to see the app has not been reviewed -- the app has not been reviewed multiple times even if they're installed from the same source.

Q. Okay. So, Professor Qian, I'll focus on something different then.

So you're an Android user; right?

A. Yes.

Q. You have a Samsung phone?

A. I now have a different phone, but I used to own a Samsung phone.

Q. What's your new phone?

A. Google Pixel 8 Pro.

Q. Okay. And you've installed apps from outside the Google Play Store before; is that right?

A. Yes.

Q. You installed some Chinese apps that, for example, don't release their apps on Play or release some sort of a watered-down version on Play; right?

A. That's right.

Q. And when that happens, you go to a Chinese website and you download it from the Chinese website; right?

A. True.

Q. And when you do that, you know which website to go to? You know which is the real authentic website; right?

A. Yes.

Q. And you personally consider the risk to be low when you download apps from those websites; right?

A. I consider it an acceptable risk, yes.

Q. An acceptable risk, right. Because it's the app's behavior and not its source that determines the security risk; right?

A. Well, I mean, the source does matter; but I agree, in general, yes, it's the behavior that matters.

Q. Yeah, the source matters. You went to the real authentic website; right? It's important to go to the real authentic website? We can agree to that; right?

A. Right.

Q. But it's the app's behavior that is the primary determinant of the risk; right?

A. Sure.

Q. So you would agree with me there are automated scans that are out there available that can review app behavior to see whether they're risky?

A. Well, automated app reviews are not sufficient; but, yes, they do exist.

Q. Malware scanning is not unique to Google. There are other third parties that can do it; right?

A. That's correct.

Q. You, yourself, have designed malware scanners in the past?

A. Yeah.

Q. And Google uses machine learning for this process; right?

A. They also have other processes, yeah.

Q. So, among other things, it will assign a score to each app telling Google exactly -- or approximately how risky the machine-learning model views the app to be from a malware perspective; right?

A. Right. They'll feed that signal to a human if needed.

Q. And then Google determines whether the app should be warned or not essentially; right?

A. I'm sorry. Can you say that again?

Q. Google will then determine whether that app should generate some sort of warning in GPP or whether it should be blocked in GPP; is that right?

A. Well, I think it's possible that a human would still need to take a look at the signals generated by the automated

systems.

Q. And if Google determines that an app is seriously problematic, Google is going to warn that app regardless of the source; right?

A. Well, they have different -- they have different ways to deal with Play apps versus off-Play apps.

Q. Let's start with Play apps.

If Google determines that an app on the Play Store is seriously problematic, it is going to reject that regardless of the source; right?

A. Well, Google Play is already the source. So I'm not sure if you can further divide it.

Q. If Google determines that an app is seriously problematic when it's going through the app review process, it is going to reject that app regardless of where the app comes from; right?

A. You mean whether it's from this developer or that developer?

MR. CLARKE: Your Honor, I'd like to show the witness, it's page 163 --

THE COURT: 163?

MR. CLARKE: -- lines 14 through 17.

THE COURT: 163:14 through 17?

MR. CLARKE: 163 of his deposition transcript, lines --

THE COURT: I'm looking at the one dated July 13.

MR. CLARKE: Professor Qian, yes, July... April 26th, Your Honor. It's possible you have a different deposition transcript.

THE COURT: One second. 163?

MR. CLARKE: Lines 14 through 17.

(Pause in proceedings.)

THE COURT: Okay. That's fine.

BY MR. CLARKE:

Q. So, Professor Qian, you testified at your deposition, you were asked (as read):

"**QUESTION:** If the app is seriously problematic, Google will reject it regardless of the source of the app; right?"

And you answered (as read):

"It is my understanding, that that is right."

Is that correct?

A. Yeah. Looking at this sentence, that's what it's saying, yes.

Q. You were asked those questions and you gave those answers?

A. Yes.

Q. And, likewise, if the app passes Google's process, then Google is going to accept it regardless of the source; right?

A. Sure.

Q. And Google also takes steps to analyze the behavior of apps that users install from off-Play sources; right?

A. I'm sorry. Can you say it again?
Q. Google also reviews the behavior of apps from off-Play sources; right?
A. Right, but they have a weaker version.
Q. And you refer to that as off-Play app review in your report?
A. Yes.
Q. Once again, that's reviewing the behavior of the app; right?
A. True.
Q. And once an app's behavior has been reviewed, it's possible to add tags or tokens to indicate that the app has been reviewed; right?
A. Well, in principle, yes.
Q. Okay. And when we say "tags or tokens," we're talking about some sort of cryptographic signature?
A. Yes.
Q. And Mac OS follows this sort of strategy of applying cryptographic signatures to apps that have been reviewed for malware; right?
A. Well, it's not reviewed, you know, in the sense that they're reviewed in Google Play Store. They're reviewed in a sense that it's scanned for any known malware or known malicious behavior without any human reviews.
Q. Professor Qian, Mac OS applies cryptographic signatures to

apps after those apps have been reviewed for malware; correct?

A. I would call it scanned instead of reviewed but, yes.

Q. You agree that after applying the cryptographic signature, Google can then turn the app back to the developer for distribution; right?

A. Yes, in principle.

Q. Okay. So you agree in principle that the process of reviewing an app can be conducted independently of the process of distributing that app; right?

A. I agree in principle, although it doesn't mean that it's a good idea to do it.

Q. In that answer did you say "I agree"?

A. Yes.

Q. Okay. In fact, Google already applies cryptographic tokens to apps which indicate that the app has been reviewed for malware; correct?

A. Again, I would not use the reviewed because it doesn't have any human or sophisticated review. I would say it's scanned but, yes.

Q. Okay. You agree that Google scans apps for malware and then applies cryptographic tokens to indicate that; right?

A. Sorry. Did you say Apple or Google?

Q. Google.

A. Sorry. Are you saying Google today does that?

Q. Yes. You agree that Google scans apps for malware and

then applies cryptographic tokens to those apps to indicate that they have been scanned; correct?

A. For Play apps or off-Play?

Q. Play apps; correct?

A. For Play apps, yes, they do get reviewed. They should be reviewed instead of scanned.

Q. And then they get tokens to indicate that they've been reviewed; right?

A. Yeah. There will be some tokens, yes.

Q. That's called frosting in Android right now?

A. Yeah, I've heard of frosting.

Q. And frosting allows those apps to then be distributed through peer-to-peer networks outside of the Google Play Store; right?

A. Yes, that's my understanding.

Q. And once those apps are downloaded onto phones, the phones check to ensure that they have the appropriate cryptographic signature; right?

A. That's what -- yes.

Q. And that's how the operating system knows that those apps have already been reviewed and that they're safe; right?

A. For the limited peer-to-peer scenario, yes.

Q. Okay. So you gave some testimony about Google Play Protect.

I would like to show you Exhibit 8007. It should be there

in your binder.

A. Yes.

Q. This is a blog post that was published about a month ago called "Enhanced Google Play Protect Realtime Scanning For App Installs." Do you see that?

A. The title up there at the top?

Q. At the top it says "Security Blog." So this blog post was retrieved from the Google Play security -- or the Android security blog. The title of the blog post is "Enhanced Google Play Protect Realtime Scanning For App Installs." Do you see that?

A. Yes, I do.

THE COURT: This is not in evidence, so take it down. Okay? You can't show things to the jury if it's not in evidence.

MR. CLARKE: So, Your Honor, this is a recent blog post that we believe has bearing on the opinions that he's reached --

THE COURT: You can just say "I'd like to admit," and then we'll see if there's an objection.

BY MR. CLARKE:

Q. Okay. Do you recognize this blog post, Mr. Qian?

A. Yes, I think so.

Q. Okay.

MR. CLARKE: I'd like to move the blog post into

evidence.

MR. OLASA: Your Honor, our objection is this postdates the reports.

THE COURT: It's sustained.

Go ahead.

BY MR. CLARKE:

Q. So, Professor Qian, do you have any understanding for whether going forward Google Play Protect is going to begin conducting realtime app installations at the time -- withdrawn.

Do you have an understanding for whether going forward Google Play Protect is going to begin conducting realtime scans, malware scans, for apps at the time that they're installed onto a device?

A. I've seen some news about it.

Q. Okay. This is a recent development; right?

A. I think it's after the -- after my report was submitted.

Q. After your report was submitted, Google announced that going forward, when Google Play Protect checks an app at the point of installation, if the app has never previously been reviewed for malware before, it is now going to do it at the time of installation; right?

A. Right. There will be some kind of realtime scanning, although I don't think human review is included. It's not the same full app review.

Q. But it is going to be scanning all apps that are installed

onto Android devices at the time of installation if they have not previously been reviewed; correct?

A. Yes.

Q. And one of the reasons that they do that is because that provides better protection against polymorphic malware; right?

A. I haven't seen the exact motivation for that, but I think it's a reasonable motivation.

Q. Okay. Now, you provided a little bit of testimony during your direct about the unknown sources warning flow; is that right?

A. Uh-huh, yes.

Q. Okay. This is a default warning on GMS devices?

A. Yes.

Q. You would agree with me that it is something that's completely decoupled from Google's scanning algorithms?

A. I'm sorry. Can you remind me the context here?

Q. Yeah. So the unknown sources warnings that you testified about in your direct examination, do you recall those?

A. Yes.

Q. Would you agree with me that those warnings are displayed in a manner that's completely decoupled from Google's scanning algorithms?

A. I think the unknown source warning is really about the permission to allow an app source to be able to install additional apps. That's what it's designed for.

Q. The unknown source warning doesn't try to distinguish between apps coming from reputable developers and spamming websites; right?

A. Right, because that's by design not the intention.

Q. It doesn't differentiate between apps that are malware and apps that are not malware; right?

A. Right. Again, that's not the intention.

Q. Okay. So a user that abandoned the workflow at the unknown sources screen, might be abandoning the installation of an app that's harmful; right?

A. Well, again, that screen is not about showing what's going to happen when you install that one particular app. It's about any number of apps that the same source can install subsequently. So I think there's a big distinction there.

Q. A user that abandons the unknown -- that abandons the installation at the unknown sources flow screen might be abandoning the installation of an app that's benign; right?

A. Possible.

Q. Okay. Or they might be abandoning the installation of an app that's risky; right?

A. Correct.

Q. Now, you cited some academic data in your report related to the malware rate of different app stores? Do you recall that data?

A. Yes.

Q. And the data used a metric called IDR or the installer detection ratio. Do you remember that?

A. Yes.

Q. So an IDR of 1 percent means that out of every 100 installations from a given app store, one of them is going to be an unwanted app; right?

A. Yeah.

Q. Okay. And when we looked at that data together in your deposition, you agreed that the Amazon Appstore is more or less equivalent to the Google Play Store in terms of malware rates. Do you remember that?

A. I don't know the exact number. I forgot. Sorry.

Q. Do you remember -- do you remember that you agreed that the Amazon Appstore is more or less equivalent to the Google Play Store in terms of malware rates?

A. I might have said it.

MR. CLARKE: May I refresh the witness with his testimony, Your Honor?

THE COURT: Go ahead.

MR. CLARKE: I'm sorry?

THE COURT: Go ahead.

MR. CLARKE: So this is deposition transcript 194, lines 18 through 25.

This should be Tab A in your binder, Professor Qian.

THE COURT: We've got 15 minutes.

MR. CLARKE: Okay. Thank you, Your Honor. I'll try and get a move on.

THE COURT: Remember, it's an antitrust case.

MR. CLARKE: Understood. Thank you, Your Honor.

THE WITNESS: I'm sorry. Can you remind me again?

BY MR. CLARKE:

Q. So deposition transcript page -- I apologize. I've now lost my page.

Deposition page 195 -- apologies. It's deposition page 194.

A. (Witness examines document.) Yes, I'm here.

Q. Okay. Do you recall agreeing that the malware rates on the Amazon Appstore are roughly equivalent to the Google Play Store?

A. Yes. I said that that's close, yes.

Q. Okay. And you would agree with me that if you wanted to go through the app installation process to actually download an app onto your phone through the Amazon Appstore, that would take what? Eight to ten friction steps in order to complete that process?

A. If you count the steps where the user's navigating on the Amazon website, yeah, probably.

Q. Okay. And you would agree with me it's a one-click process from the Google Play Store?

A. Roughly, yes.

Q. Okay. And those are for two different app stores that have roughly the same risk when it comes to malware; correct?

A. According to the data presented in this paper, yes.

Q. Okay. You're familiar -- you testified on your direct about centralized notarization; is that right?

A. Yes.

Q. And in centralized notarization, Google could open its review service to apps intended for distribution via non-Play Store mechanisms; right?

A. I'm sorry. Can you say it again?

Q. In centralized distribution, Google could open up its review service to third parties; right?

A. Yes, it could open it up to any developers.

Q. And that's an opt-in framework; right? Developers aren't forced to submit their apps to Google under that scenario?

A. That's correct.

Q. Okay. Do you know whether Google has ever actually looked at a system for third parties to submit apps directly to Marmit for review?

A. For Marmit, yes, I've heard of that.

Q. You have heard of that?

A. I believe we talked about it during my deposition.

MR. CLARKE: Your Honor, I'd like to show the witness deposition page 177, lines 2 through 6.

THE COURT: Let's not rehash depositions. Okay?

Let's just focus on in-court exam. You can use a deposition to impeach, but let's not talk about a party that none of us are invited to but you two.

Okay. What line is that?

MR. CLARKE: So I'd like to impeach the witness with page 177, lines 2 through 6, Your Honor.

THE COURT: Okay.

BY MR. CLARKE:

Q. So you were asked (as read):

"QUESTION: Do you have any understanding for whether Google has ever looked at a system for third parties to submit apps directly to Marmit for review?"

And you said (as read):

"ANSWER: I was not aware of that."

Correct?

A. I'm sorry. I think I was saying that during the deposition, you brought this up, and that's how I became aware.

Q. You learned of it through the course of the deposition, I understand.

So you weren't aware of it at the time that you formed your opinions that centralized notarization is inappropriate; right?

A. Correct.

Q. Because that's not something you looked into when you were formulating your opinions about centralized notarization;

right?

A. That's correct.

Q. Okay. So you didn't look into this issue, you didn't ask anybody to see any documents related to this question; right?

A. No.

Q. So I'd like to take a look at Exhibit 8577. This is a document titled "Third-Party Web App Scanning Service PRD." Do you see that?

A. Yes.

Q. Okay. Have you ever seen this document before?

A. Let me take a quick look.

(Witness examines document.) No, I don't think I've seen it before.

Q. So this isn't something that you were aware of at the time you formulated your opinions in this case; right?

A. That's right.

Q. If you look at page 2, there's a paragraph that says (as read):

> "Solution overview and benefits provide off-market stores, third-party providers, and OEMs with web services where they can submit apps and ROMs to be scanned against a database of known malware signatures and vulnerabilities."

Do you see that?

A. Yes.

Q. So this is a proposal to make Marmit available to third parties; right?

A. I guess it didn't mention Marmit specifically in this sentence, but it seems plausible.

Q. Well, if you take a look a little bit --

THE COURT: Do you know one way or the other? Do you know? We're not here for guesses or plausibility. Do you know for sure one way or the other? If you don't, you can just say "I don't know."

THE WITNESS: I'm not exactly sure.

THE COURT: All right. Next question.

BY MR. CLARKE:

Q. You don't know one way or the other.

Do you have any idea why Google might be reluctant to make Marmit available for third parties?

A. I believe you showed some internal e-mails during my trans -- during my deposition.

Q. And you agreed with me when we looked at those --

THE COURT: I really -- we're going to stop here. Don't refer to your deposition. Okay? Just, we can only deal with the evidence that's admitted here in court; and these side things that happened before, don't refer to them. The lawyer may show it to you, that's perfectly fine, otherwise don't refer to it.

So let's ask that question again, and try to answer it to

the best of your ability without mentioning anything else outside of the courtroom.

BY MR. CLARKE:

Q. Let me -- maybe I can try and ask it a little bit differently.

Do you agree with me that competitive reasons might play a role in Google's decision not to make Marmit available to third parties?

A. Yes. I think security is -- you know, you can -- there can be a lot of intellectual property included in, you know, the security technologies. I think it's reasonable.

Q. Okay. You provided some testimony about scalability of centralized notarization. Do you recall that?

A. Yes.

Q. Do you have any understanding -- just yes or no -- for how many reviewers Google actually has assigned to the off-Play review queue?

A. No, I don't know the exact number.

Q. So if I told you that there was only one reviewer that was assigned to the off-Play review queue in 2019, you wouldn't have any basis to dispute that?

A. I don't have any data to say yes or no.

Q. Do you have any understanding for what the actual review coverage was that that one reviewer was able to achieve in 2019?

A. No, I don't have any data.

Q. Okay. You agree with me that if Google only had one reviewer assigned to the off-Play review queue, it could triple or quadruple it's review volume by hiring two or three people; right?

A. Potentially.

Q. Okay.

THE COURT: Okay. Disregard that. He doesn't know. Next question, please. You need to ask something that he actually has some knowledge about. Okay?

MR. CLARKE: Understood, Your Honor.

THE COURT: You've got five minutes, and then I'm going to see if there's any redirect.

MR. CLARKE: Thank you, Your Honor.

BY MR. CLARKE:

Q. Professor Qian, you were asked some questions about a warning screen that's displayed by Epic; right?

A. Yes.

Q. Okay. You recall that; right?

A. Yes, I recall.

Q. You do have personal knowledge about that warning screen; right?

A. I'm sorry?

Q. You do have knowledge about that warning screen; right?

A. I've seen that screen.

Q. Okay. That came from your expert report. Do you recall that?

THE COURT: How about this: Rather than asking what he remembers, just ask a question. Okay?

MR. CLARKE: Okay. Thank you, Your Honor.

BY MR. CLARKE:

Q. That image that you created was created on August 2018; is that right?

A. Sounds about right. I'm not 100 percent sure.

Q. And isn't it true that prior to September of 2018, the permission for installing apps from unknown sources was not controlled on a per-source basis on Android?

A. I don't remember the exact date, but according to that screen, it actually says "Your browser has been granted some special permission." So it sounds like it's specific to browser.

Q. And at that time, the unknown sources permission was a global permission on Android; right?

A. I don't know for sure.

Q. You don't know one way or the other whether it was a global permission?

A. (No audible response.)

Q. If Epic had decided to display that screen in response to a global permission as opposed to a per-source permission, would that change your opinion with respect to that screen?

A. No, because it's still showing that sideloading is risky.

Q. Okay. If there were a unique -- withdrawn.

MR. CLARKE: Your Honor, I have no further questions.

THE COURT: Okay. Very brief redirect.

MR. OLASA: We have no questions, Your Honor.

THE COURT: All right. Great.

You can step down. Thanks for coming in. Be careful on the way down.

(Witness excused.)

THE COURT: All right. We're going to adjourn. We're not coming in tomorrow. Okay? You can if you want, but we won't be here.

See you Monday morning at 9:00. Now, remember, next Friday, let's plan on it. Okay? I'm going to talk with the lawyers. Both sides are making efficient good progress. I'm going to check in with them so I can give a little more of an update on Monday, what the timeline looks like.

So this is the perfect time to put everything out of mind. Enjoy the next couple of days. Whatever you're going to do, quiet reflection, family, whatever it is, just have a good time. Put all this out of your mind. No research. No investigation. Don't look anybody up. Don't look anything up. Don't look any concepts up.

And I'll see you on Monday morning.

THE CLERK: All rise.

(Proceedings were heard out of the presence of the jury:)

THE COURT: Okay. I think we should be able to finish by next Friday.

MR. BORNSTEIN: So on the Epic side, Your Honor, we have -- and really the both of us, we have two pairs of experts to come. After the security experts, we have the accounting folks --

THE COURT: The economists and --

MR. BORNSTEIN: The accounting folks will come first. They should both be very short.

We have about a half an hour altogether of fact deposition from finance people that we need to get in before the accountants testify.

THE COURT: All right.

MR. BORNSTEIN: I would expect all of that to be able to be done before the lunch break, if not sooner, on Monday.

THE COURT: Good. Okay.

MR. BORNSTEIN: And then we have the --

THE COURT: That's it for the experts then; right?

MR. BORNSTEIN: No. Then we have the economists.

THE COURT: Oh, then economists. Okay. Right.

MR. BORNSTEIN: Yeah.

THE COURT: Okay. That will be Monday afternoon?

MR. BORNSTEIN: It will probably go a little longer than Monday afternoon.

THE COURT: They're going to start Monday afternoon.

MR. BORNSTEIN: We should be able to start Monday afternoon, yes.

THE COURT: Okay. If I may just give you a word, you're all experienced, but this was way too much time on security. Way too much time.

Help your economists focus. They're usually very good at it, and it's much more antitrustty, so I'm confident.

But let's not do this again. I'm talking about both sides. This is a bilateral suggestion. Okay?

All right. Okay. Let's get this done by Friday, huh?

MR. POMERANTZ: I don't know, Your Honor. I mean, I don't know how long the economists will take. We do have some witnesses to put on thereafter.

THE COURT: How many, roughly, are you -- I'm not tying your hands, but how many, roughly, do you expect?

MR. POMERANTZ: I think live witnesses there may be -- I'm looking here now -- maybe five or six.

THE COURT: Okay. Is that mainly on the counterclaims or --

MR. POMERANTZ: No, no. These are fact witnesses on our side.

THE COURT: Oh.

MR. POMERANTZ: Okay. So I guess in terms of live witnesses, we're expecting three Google witnesses, two Epic

witnesses, and one third party, which is Apple.

THE COURT: All right.

MR. POMERANTZ: And so those three -- those six live witnesses, and then we'll have some deposition testimony, which will be relatively short.

THE COURT: Look, we're at the point now where we have a lot in the hopper. Okay? So we do not need someone to say "This is what MADA means." Okay? We don't need to go through the 19 screens. We don't need to go through, you know, "Spotify pays X percent and Amazon pays Y percent, but I pay 30 percent." That's all in.

All right. So I'm going to start -- it's getting quite cumulative, and I've given you -- you've both given each other some leeway, I've given you some leeway, but we've got to get going now. We're going to start losing some people, and it's just -- we've got to get going.

Just be prepared. I'm going to be a little bit more sharp next week on not going over something we've heard three times before. All right?

MR. BORNSTEIN: Understood, Your Honor.

The one thing that we have, which is important to us, is just to make sure after Google finishes its case, we can have the opportunity for a very brief rebuttal, which I think may be necessary from the economists.

THE COURT: Well, I don't know. I'm not making any

promises. All right?

Also, you're getting really short on time.

MR. BORNSTEIN: I understand, Your Honor. We are reserving time just for that purpose.

THE COURT: Well, shoot, I forgot to ask the final time count.

Are you able to do that, Ms. Clark, or is it too much for right now?

THE CLERK: I don't have the final.

THE COURT: All right. I'll tell you on Monday morning. Okay? But we should be able to accelerate the pace significantly at this point.

MR. BORNSTEIN: If I could be --

THE COURT: Make everything new and fresh next week. If it's not, I'm probably going to ask you to stop because we've heard a lot about the same stuff.

MR. BORNSTEIN: Understood, Your Honor.

If I could say one word on the rebuttal, I actually think it would expedite the presentations because we could have our opening presentations not have to anticipate the 600 pages of reports that we have from the defendants -- from Google; and we can have a concise opening presentation without having to talk about all the things that might come up, which Google might not actually present, and then we can have our rebuttal focus just on the things that actually came in evidence.

THE COURT: In theory, that seems promising.

MR. BORNSTEIN: Thank you, Your Honor.

THE COURT: But don't -- that's not a guarantee. Okay? All right. Not judge estoppel. You can't come back later and say "You promised me."

MR. BORNSTEIN: I hear Your Honor very clearly.

THE COURT: Okay. Anything else we need to do before next week?

MR. POMERANTZ: I don't think so, other than have a Happy Thanksgiving.

THE COURT: Yes, that's my line.

MR. POMERANTZ: I'm sorry, Your Honor.

THE COURT: Just wait for a moment.

Anything else for next week?

MR. BORNSTEIN: We are working on one issue, Your Honor, that I hope we don't need to bring to you. Just, it's the matter we talked about on that one finance document where we had believed that we put in appropriate foundation through the CFO.

THE COURT: I assume that was the half hour you were mentioning. It's not?

MR. BORNSTEIN: No, we have a little bit of deposition testimony from the CFO and from one of her reports, which is really just to get in the documents. I mean, if we can find another way to get the documents just so the accountants can

talk about them, that would expedite things.

THE COURT: All right. So are you still chatting about that?

MR. POMERANTZ: Yes, Your Honor.

THE COURT: Okay. All right. I'm actually pretty confident we can probably wrap it up by next Friday, and I really would like to target that. Okay? I mean, I'm not going to jam anyone, but let's target that.

All right. Everyone is going to go do something? You're in LA. You can go home.

MR. POMERANTZ: I am, Your Honor.

THE COURT: New York, what are the New Yorkers going to do?

MR. BORNSTEIN: I have to go home for personal reasons, Your Honor. We've all got our plans.

THE COURT: All right. Good.

All right. I'll see you on Monday. Have a good break.

MR. BORNSTEIN: Thank you, Your Honor.

THE CLERK: All rise. Court's in recess.

THE COURT: Oh, final jury instructions. You're filing those tomorrow; right? And then we're going to have to get cracking on those.

Oh, and a new verdict form too. All right. You're doing both of those? If you didn't do the verdict form, you can have until next week; but you're doing the -- you're revising the

jury instructions, didn't we talk about tomorrow?

MR. BORNSTEIN: We did talk about the jury instructions, Your Honor.

THE COURT: Okay. Good.

Okay. Great. Thanks.

(Proceedings adjourned at 3:31 p.m.)

---oOo---

CERTIFICATE OF REPORTER

I certify that the foregoing is a correct transcript from the record of proceedings in the above-entitled matter.

DATE: Tuesday, November 21, 2023

Kelly Shainline, CSR No. 13476, RPR, CRR
U.S. Court Reporter